

De Perfect Storm

Nederlandse & Europese Compliance 2024-2028
Hoe meer dan twintig wetten tegelijkertijd uw organisatie raken — en wat er sinds april is veranderd.

€20M	8.000+	15 aug	72u
max. AVG-boete per overtreding	organisaties nu onder de Cbw	Cbw & Wwke van kracht, 2026	om datalekken te melden

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 — en sinds de eerste editie van dit whitepaper (april 2026) is de storm niet gaan liggen. Hij is geland.

"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. 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.

Wat is er veranderd sinds editie 1 (april 2026)? Het belangrijkste: de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten zijn niet langer "verwacht" — ze zijn wet, aangenomen door de Eerste Kamer op 7 juli 2026, en treden op 15 augustus 2026 in werking. Zonder overgangsperiode. Daarnaast is de hoog-risico AI Act-verplichting uitgesteld naar december 2027, is er een nieuw en omstreden Brussels dossier bijgekomen (de Digital Omnibus), en is de geopolitieke context sinds februari verder geëscaleerd. Deze editie loopt alle deltas na.

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. 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 — en, zoals sectie 4.10 laat zien, een keuze die in Brussel zelf nu onder druk staat.

Dit document geeft geen stappenplan en beveelt geen leveranciers aan. Het biedt een overzicht van wat er speelt, onderbouwd met geverifieerde bronnen uit het EU Official Journal, CBS, ENISA, NCSC, Rijksoverheid, 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.

Executive Summary

Nederlandse en Europese organisaties staan voor een ingrijpende compliance-situatie. In de periode 2024-2028 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 — en met de inwerkingtreding van de Cbw en Wwke op 15 augustus 2026 is die verandering niet langer toekomstmuziek.

De wetten die nu van kracht zijn of 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 — status per augustus 2026

Kader	Datum	Status
DORA	17 jan 2025	Van kracht, geen overgangsperiode. Art. 28 ICT-derdepartijregister sinds 17 jan 2026.
AI Act geletterdheidsplicht + verboden praktijken	2 feb 2025	Van kracht voor alle organisaties die AI inzetten. Tekst versoepeld per 27 juli 2026.
AI Act transparantieplicht (art. 50)	2 aug 2026	NIEUW VAN KRACHT Chatbot-melding, AI-content labeling.
CRA — in werking / rapportageplicht	10 dec 2024 / 11 sep 2026	In werking; rapportageplicht kwetsbaarheden nadert (nog geen vertraging).
Cyberbeveiligingswet (Cbw)	15 aug 2026	VAN KRACHT Aangenomen Eerste Kamer 7 juli 2026. Geen overgangsperiode. ~8.000 organisaties.
Wet weerbaarheid kritieke entiteiten (Wwke)	15 aug 2026	VAN KRACHT Gelijktijdig met Cbw aangenomen. ~500 organisaties extra aangewezen.
BIO2 v1.3	5 mrt 2026	Gepubliceerd; wettelijk verankerd via Cbw-ministeriële regeling vanaf 15 aug 2026.
NEN 7510:2024	16 dec 2024	Gepubliceerd; zorgsector in transitie, deadline gecertificeerde organisaties 20 feb 2027.
AI Act hoog-risico (Bijlage III)	2-aug-2026	UITGESTELD naar 2 december 2027 (Digital Omnibus on AI, Vo. 2026/1744).

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.

Nieuw sinds editie 1: het EU Digital Omnibus-pakket (AVG/AI Act/Data Act-versoepeling) is het meest omstreden Brusselse dossier van 2026 geworden — het Nederlandse kabinet heeft er in juni 2026 formeel bezwaar tegen aangetekend. Zie sectie 4.10.

De Vierde Kracht — Economische Onzekerheid

De compliance-golf treft organisaties in een periode van structurele economische tegenwind. De bredere Nederlandse arbeidsmarkt is in de loop van 2026 wel afgekoeld (CBS: vacaturegraad daalt, spanning neemt af — 91 vacatures per 100 werklozen in Q1 2026, tegenover een structureel tekort in eerdere jaren), maar dat biedt organisaties geen adempauze op de compliance-vraag: ICT-, cybersecurity- en AI-governance-rollen blijven structureel schaars, ook nu de brede arbeidsmarkt verzacht (zie sectie 10). Investeringsparadox blijft onverminderd van kracht: compliance-investeringen zijn verplicht en niet uitstelbaar, terwijl budgetdruk bij precies die bedrijven het hoogst is.

Sector Urgentie Heatmap — 13 Kernsectoren

Onderstaande matrix dekt de 13 kernsectoren uit de oorspronkelijke HCI-analyse. Let op: de Cbw zelf is per 15 augustus 2026 van toepassing op **18 sectoren** (waaronder ook drinkwater, ruimtevaart en afvalwaterbeheer, niet los uitgesplitst in deze matrix). Rood = directe actie vereist. Oranje = voorbereiding lopend jaar noodzakelijk. Geel = in kaart brengen. Grijs = relatief beperkte impact.

Sector	NIS2/Cbw	DORA	AVG	AI Act	BIO2	NEN 7510	CER/Wwke	CRA
Overheid / Gemeente	KRITIEK	LAAG	HOOG	KRITIEK	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: van kracht per 15 juli 2026 → gecorrigeerd naar 15 augustus 2026. DORA: van kracht per 17 jan 2025. CRA: volledig van kracht 11 dec 2027 (rapportageplicht al sept. 2026). BIO2: wettelijk verankerd per 15 aug 2026 (Cbw-ministeriële regeling).

Financiële Impact — Wat staat er op het spel?

Boetes zijn geen theoretisch risico meer. Cumulatieve GDPR-boetes in de EU zijn inmiddels opgelopen tot ruim **€7,1 miljard** (cumulatief sinds 2018, stand medio 2026) — een forse stijging ten opzichte van de €2,1 miljard die in 2023 alleen al werd opgelegd. De Autoriteit Persoonsgegevens zelf profileert zich in 2026 nadrukkelijk als een steviger handhaver, met een groter budget en meer capaciteit. DORA introduceert eigen boetekaders boven op de bestaande AVG-structuur, en met de Cbw komt daar per 15 augustus 2026 een vierde meldplicht-regime bij.

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	15 aug 2026 ✓
CRA	€15M of 2,5% wereldwijde omzet	Software/hardware-aanbieders	Aangewezen markttoezichthouder	Dec. 2024 ✓ (rapportage sep 2026)
EU AI Act (hoog-risico)	€30M of 6% wereldwijde omzet	Hoog-risico AI-systemen	Nog aan te wijzen NL	Uitgesteld → dec. 2027
EU AI Act (overig / transparantie)	€15M of 3% wereldwijde omzet	Overige overtredingen, incl. art. 50	Nog aan te wijzen NL	Feb. 2025 / 2 aug 2026 ✓
CER / Wwke	Bestuurdersaansprakelijkheid	Kritieke entiteiten	NCTV / vakdepartement	15 aug 2026 ✓

Rekenvoorbeeld: Ziekenhuis met ransomware-incident

Stel: een middelgroot ziekenhuis (250 bedden, jaaromzet €120M) wordt getroffen door ransomware. Patiëntgegevens lekken. NIS2/Cbw én AVG zijn van toepassing — sinds 15 augustus 2026 geen theoretisch scenario meer, maar een direct toepasselijk wettelijk regime. De instelling heeft geen ISMS, geen meldproces.

- 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.

De Kernkaders — Kort & Concreet

4.1 NIS2 / Cyberbeveiligingswet (Cbw) — van kracht sinds 15 augustus 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 met bijna twee jaar. De Eerste Kamer nam de Cbw en de Wwke op **7 juli 2026** aan; beide wetten traden op **15 augustus 2026** in werking, zonder overgangperiode. De wet geldt voor ruim **8.000 organisaties in 18 sectoren** — bijna een vertienvoudiging ten opzichte van de ~1.000 organisaties die eerder onder de Wbni vielen.

Kernverplichtingen: registratie bij NCSC (mijn.ncsc.nl), risicobeheer, supply chain security, incidentbeheer, MFA, encryptie, trainingsplicht bestuurders. Meldplicht significant incident: 24u vroegtijdige waarschuwing → 72u vervolgmelding → 1 maand eindverslag bij NCSC. Organisaties moeten daarnaast hun eigen klanten informeren bij een significant incident (informatieplicht).

Geen overgangperiode betekent: vanaf 15 augustus gelden alle verplichtingen op dag één. Veel organisaties ontdekken nu voor het eerst dat ze — via de toeleveringsketen van een essentiële of belangrijke entiteit — binnen de reikwijdte vallen, ook zonder zelf formeel te zijn aangewezen.

4.2 DORA — van kracht 17 januari 2025

DORA (Verordening EU 2022/2554) is rechtstreeks toepasselijk in de financiële sector. Vijf pijlers: ICT-risicobeheer, incidentrapportage, TLPT (penetratietests voor grote instellingen), third-party ICT-register (art. 28, verplicht sinds 17 januari 2026), informatie-uitwisseling. Boete: tot 2% jaaromzet. DORA is lex specialis t.o.v. NIS2/Cbw voor de financiële sector.

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

De AVG blijft de basiswet voor persoonsgegevensverwerking. De AP is in 2026 nadrukkelijker gaan handhaven, met meer budget en capaciteit. In december 2025 bevestigde het kabinet dat de US CLOUD Act van toepassing is op Microsoft 365, Teams en Zivver. Geen reden om morgen over te stappen, maar wel een aanleiding om het exit-scenario voor kritieke leveranciers — contractueel vaak verplicht, in de praktijk zelden getest — serieus te nemen. Zie ook sectie 4.10: de AVG zelf ligt via het Digital Omnibus-pakket onder vuur.

4.4 EU AI Act — hoog-risico verplichtingen uitgesteld, transparantie is nu wél hard recht

Datum	Verplichting
2 feb 2025 ✓	Verbod onaanvaardbaar-risico AI + AI-geletterdheidsplicht (art. 4) — al van kracht, tekst versoepeld per 27 juli 2026
2 aug 2025 ✓	Verplichtingen GPAI-modellen (grote taalmodellen)
2 aug 2026 ✓	Transparantieplicht art. 50 van kracht — AI-content labeling, chatbot-melding, machine-leesbare markering. Geldt voor elk bedrijf dat AI-systemen inzet richting EU-gebruikers.
2 dec 2026	Watermerkplicht voor AI-content die vóór 2 aug 2026 al op de markt was
2-aug 2026	UITGESTELD Volledige verplichtingen hoog-risico AI, stand-alone systemen (Bijlage III) → nu 2 december 2027
2-aug 2027	UITGESTELD Hoog-risico AI ingebed in gereguleerde producten (Bijlage I) → nu 2 augustus 2028

Het uitstel komt uit de Digital Omnibus on AI (Verordening (EU) 2026/1744, gepubliceerd 24 juli 2026, van kracht 27 juli 2026) en is toegekend omdat de noodzakelijke technische standaarden en richtsnoeren nog niet klaar waren. **Belangrijk:** de onderliggende verplichtingen zijn niet geschrapt, alleen uitgesteld — en organisaties die hoog-risico AI bouwen of inkopen (recruitment, kredietbeoordeling, medische triage) doen er goed aan nu al te beginnen, omdat conformiteitsbeoordeling en kwaliteitsmanagementsystemen 9-12 maanden voorbereiding vragen. De transparantieplicht van 2 augustus 2026 daarentegen schuift niet en raakt vrijwel elke organisatie die een chatbot inzet of AI-gegenereerde content publiceert — inclusief marketing- en outreach-content.

4.5 BIO2 — wettelijk verankerd per 15 augustus 2026

BIO2 v1.3 (gepubliceerd in de Staatscourant op 5 maart 2026) vervangt BIO 1.04 voor het Rijk, provincies en waterschappen, en geldt sinds september 2025 al als verplichtende zelfregulering voor diezelfde lagen. Met de inwerkingtreding van de Cbw wordt BIO2 via de ministeriële Cyberbeveiligingsregeling sector Overheid het formele, wettelijk verankerde normenkader waarmee overheidsorganisaties hun zorgplicht invullen. Gemeenten hanteren BIO 1.04zv nog als verplichtend, met BIO2 als richtinggevend kader. BIO2 vereist een ISMS op basis van ISO 27001 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 introduceert 93 algemene en 8 zorgspecifieke beheersmaatregelen. Verplichte encryptie van patiëntgegevens is nieuw. Gecertificeerde organisaties moeten uiterlijk 20 februari 2027 getransitioneerd zijn. IGJ eist aantoonbare voldoening; NEN 7510 vult de NIS2-zorgplicht in maar dekt niet de meld- en registratieplicht volledig.

4.7 CER / Wwke — van kracht sinds 15 augustus 2026

De Wet Weerbaarheid Kritieke Entiteiten implementeert de CER-richtlijn (EU 2022/2557) en trad gelijktijdig met de Cbw in werking. Complementair: Cbw = digitale weerbaarheid, Wwke = fysieke weerbaarheid. Van toepassing op elf sectoren kritieke infrastructuur; ongeveer 500 organisaties worden vanaf 15 augustus 2026 formeel aangewezen als kritieke entiteit. Na aanwijzing: 10 maanden om te voldoen.

4.8 CRA (Cyber Resilience Act) — tijdelijk ongewijzigd, guidance gepubliceerd

Geen vertraging: de rapportageverplichting voor actief misbruikte kwetsbaarheden en ernstige incidenten (art. 14) blijft staan op **11 september 2026**, via het Single Reporting Platform van ENISA (art. 16), dat momenteel functioneel en beveiligingstesten doorloopt. Op 27 juli 2026 heeft de Europese Commissie bovendien haar officiële toepassingsguidance gepubliceerd (document C(2026) 5252, ~80 pagina's, gericht op MKB-toepasbaarheid). Volledige toepassing (CE-markering, conformiteitsbeoordeling): 11 december 2027. Pure SaaS/PaaS blijft buiten scope; embedded software/firmware valt wel onder de CRA. 90% van producten kan zichzelf certificeren (self-assessment).

4.9 Aanvullende Sectoren — Buiten de Kernacht

Farma & Life Sciences, Telecom & ICT-dienstverleners, Maakindustrie/OEM, Pensioenfondsen & Verzekeraars en Detailhandel vallen eveneens onder de beschreven wetgeving. Voor deze vijf sectoren geldt onverkort wat in editie 1 beschreven stond — geen wijzigingen sinds april 2026 die de sectorspecifieke analyse raken, met uitzondering van de algemene Cbw/AI Act-deltas hierboven.

4.10 Digital Omnibus — het nieuwe, omstreden dossier NIEUW IN EDITIE 2

Dit dossier ontbrak in editie 1 en verdient nu een eigen plek: het is het meest omstreden EU-wetgevingstraject van 2026 geworden. Gepresenteerd door de Europese Commissie op 19 november 2025 onder de vlag van "administratieve vereenvoudiging", beoogt het pakket de AVG, de AI Act, de Data Act en het ePrivacy-kader te herzien.

- **Wat verandert er mogelijk:** een versmalling van het begrip 'persoonsgegevens' en 'pseudonimisering' (data die praktisch niet te herleiden is, zou buiten de AVG kunnen vallen — ook voor AI-training); een verruiming van de meldtermijn voor datalekken van 72 naar 96 uur bij hoog-risico-incidenten; een nieuwe grondslag om persoonsgegevens zonder toestemming te gebruiken voor AI-training op basis van "gerechtvaardigd belang"; de AI Act hoog-risico-vertraging (zie 4.4) is er onderdeel van.
- **Kritiek:** EDPB en EDPS (Europese privacytoezichthouders) waarschuwen publiekelijk dat de voorgestelde definitiewijziging het begrip persoonsgegevens fundamenteel kan uithollen. Het Nederlandse kabinet — staatssecretarissen Aerdts (EZK) en Van Bruggen (JenV) — stuurde in juni 2026 een formele Kamerbrief met de waarschuwing dat het voorstel op cruciale punten de privacybescherming en de werking van de AVG dreigt te ondermijnen.
- **Status:** trilooffase gaande op EU-niveau; definitieve goedkeuring wordt niet eerder dan eind 2026 verwacht. Het AI Act-gedeelte (hoog-risico-uitstel) is al wél definitief en van kracht (zie 4.4).

Relevantie voor uw AVG-positionering: een deel van de druk achter dit dossier komt van Amerikaanse Big Tech-lobby richting eenvoudigere AI-datatoegang. Voor organisaties die bewust kiezen voor AVG-compliant, EU-gesourcete data blijft de onderliggende rechtsonzekerheid een reden om nu al hogere interne standaarden te hanteren dan het wettelijk minimum dat er mogelijk uitkomt.

Volledig Wetgevingslandschap — Alle Kaders

De negen 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. Wijzigingen ten opzichte van editie 1 zijn gemarkeerd.

A — Reeds behandeld (kernkaders)

Kader	Type	Van kracht	Sectie
NIS2 / Cyberbeveiligingswet (Cbw)	EU richtlijn → NL wet	15 aug 2026 ✓	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 2025–2028	4.4
BIO2	NL norm / wettelijk verankerd	5 mrt 2026 / 15 aug 2026	4.5
NEN 7510:2024	NL norm (wettelijk)	16 dec 2024 ✓	4.6
CER / Wwke	EU richtlijn → NL wet	15 aug 2026 ✓	4.7
CRA	EU verordening	10 dec 2024 ✓	4.8
Digital Omnibus	EU verordening (in triloog)	Deels van kracht (AI-uitstel), rest eind 2026+	4.10

B — Aanvullende EU-verordeningen (rechtstreeks werkend)

Kader	Van toepassing	Kern
Data Act	12 sept 2025 ✓	Toegang tot en gebruik van data van connected devices. Verplichte datadeling met overheid bij noodgevallen.
Data Governance Act (DGA)	24 sept 2023 ✓	Kader voor data-intermediairs, Europese dataruimtes (Health Data Space e.a.).
Digital Markets Act (DMA)	2 mei 2023 ✓	Verplichtingen voor gatekeepers (Alphabet, Apple, Meta, Microsoft, Amazon, ByteDance).
Digital Services Act (DSA)	17 feb 2024 ✓	Aansprakelijkheid online platforms, aanbevelingsalgoritmen, advertentietransparantie.
eIDAS 2.0	20 mei 2024 ✓ (impl. 2026)	Europese digitale identiteitsportemonnee, verplichte acceptatie publieke diensten.
MiCA	30 dec 2024 ✓	Regulering crypto-activa, vergunningplicht CASPs.
Product Liability Directive (herzien)	Aangenomen 9 nov 2024 (impl. 2026)	Uitbreiding aansprakelijkheid naar software, AI-systemen en digitale diensten.

C — In nationale implementatie / D — In voorbereiding

Kader	Status (aug 2026)
CSRD	Gefaseerd 2024–2028; grote bedrijven rapporteren over FY2024/2025
PSD3 + PSR	In voorbereiding, verwacht van toepassing 2027
ePrivacy Regulation	Nog altijd geblokkeerd; onderdeel van Digital Omnibus-discussie, geen concrete datum
EHDS (European Health Data Space)	Gefaseerde toepassing 2027–2030
EUCS (EU Cloud Cert. Scheme)	Verwacht 2026–2027, nog geen definitieve goedkeuring
Cyber Solidarity Act	Aangenomen april 2024, implementatie 2025–2026 loopt

Sectie E (NL-specifieke kaders: Wdo, UAVG, Wiv 2017, Algoritmeregister, ENSIA, Wbb) en sectie F (ISO/NEN-normen als compliance-instrument: ISO 27001/27002/42001/27701/62443 e.a.) zijn ongewijzigd ten opzichte van editie 1.

Samenloop in de Praktijk — Vier Scenario's

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

Een aanvaller versleutelt het EPD-systeem. Patiëntgegevens zijn tijdelijk niet beschikbaar en er is een vermoeden van dataexfiltratie. Sinds 15 augustus 2026 is dit geen hypothetisch scenario meer, maar direct toepasselijk recht.

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): hoog-risico AI-systeem. **Update editie 2:** de zwaarste verplichtingen (conformiteitsbeoordeling, risicomanagementsysteem, EU-registratie) zijn uitgesteld naar 2 december 2027 — maar de transparantieplicht naar sollicitanten (art. 50) geldt al sinds 2 augustus 2026, en de AVG-verplichtingen (DPIA, art. 22 profilering) golden al langer en blijven onverkort van kracht. De uitgestelde deadline is geen reden om te wachten: conformiteitsbeoordeling kost 9-12 maanden voorbereiding.

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

Een middelgrote bank maakt gebruik van een US-based cloud provider voor kernbankieren-functionaliteit. DORA art. 28 vereist een uitgebreid ICT-derdepartijregister — sinds 17 januari 2026 verplicht, dus inmiddels een lopende verplichting, geen aankomende. Het kabinet bevestigde in december 2025 dat de US CLOUD Act van toepassing is op Microsoft 365 en Teams. De vraag die hier echt gesteld moet worden: wanneer heeft uw organisatie voor het laatst het exit-scenario voor uw cloud-leveranciers geactualiseerd en getest?

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

Een Nederlandse SaaS-aanbieder biedt een platform aan met een hardware-gateway (IoT-device). De gateway valt onder CRA. Deadlines ongewijzigd: rapportageplicht kwetsbaarheden per 11 september 2026, CE-markering per 11 december 2027. Tegelijk kan het platform sinds 15 augustus 2026 onder de Cbw vallen als het als 'digitale infrastructuur' kwalificeert — met eigen registratie- en meldplicht, los van de CRA-verplichtingen.

07

Bestuurdersaansprakelijkheid — Persoonlijk Risico

Een van de meest onderschatte aspecten van de Perfect Storm is de verschuiving naar persoonlijke aansprakelijkheid van bestuurders. Met de Cbw en Wwke nu daadwerkelijk van kracht, is dit niet langer een toekomstig risico maar een lopende verplichting.

Kader	Wat vereist wordt
NIS2 / Cbw	Bestuurders moeten cyberbeveiligingsmaatregelen goedkeuren, toezicht houden en aantoonbaar voldoende kennis hebben (trainingsplicht). Persoonlijke aansprakelijkheid, van kracht sinds 15 aug 2026.
CER / Wwke	Bestuurdersaansprakelijkheid bij ernstige niet-naleving. Sancties in wet opgenomen, van kracht sinds 15 aug 2026.
AVG	Organisaties (en feitelijk leidinggevend) kunnen aansprakelijk worden gesteld. Boetes niet fiscaal aftrekbaar (NL beleid).
DORA	Bestuur is eindverantwoordelijk voor ICT-risicobeheer. Jaarlijkse evaluatie vereist. DNB kan bestuurders persoonlijk aanspreken bij systematisch falen.
AI Act	Organisaties die verboden AI inzetten riskeren de hoogste boetes. Geen 'wist niet'-verweer na feb. 2025 — geletterdheidsplicht geldt, in versoepelde vorm sinds 27 juli 2026.

Drie concrete acties voor het bestuur — nu

- Laat een formeel besluit nemen in de RvB/MT dat het cyberbeveiligingsbeleid is goedgekeurd — dit is nu een actieve Cbw-verplichting, geen best practice meer.
- Volg of organiseer een aantoonbare AI-geletterdheidsmodule voor bestuurders en management.
- Zorg dat uw CISO of externe compliance-adviseur periodiek aan het bestuur rapporteert over compliance-status en leg dit vast in de notulen — inclusief het registratiestatus bij NCSC.

Kritieke Deadlines 2024-2028

Datum	Mijlpaal	Kader	Wie
17 jan 2025 ✓	DORA van kracht — geen overgangsperiode	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 gepubliceerd	BIO2	Overheid
27 jul 2026 ✓	Digital Omnibus on AI van kracht — hoog-risico AI uitgesteld	EU AI Act	Alle organisaties
2 aug 2026 ✓	AI Act transparantieplicht (art. 50) van kracht	EU AI Act	Alle AI-gebruikers
15 aug 2026 ✓	Cyberbeveiligingswet + Wwke van kracht — geen overgangsperiode	NIS2 / CER	Alle sectoren (~8.500 org.)
11 sep 2026	CRA rapportageverplichting kwetsbaarheden (ENISA)	CRA	Software/hardware-aanb.
2 dec 2026	Watermerkplicht AI-content die vóór 2 aug 2026 al op de markt was	EU AI Act	AI-content-aanbieders
20 feb 2027	NEN 7510:2024 transitie — deadline gecertificeerde org.	NEN 7510	Gecertificeerde zorgorgan.
~~2 aug 2027~~	(vervallen, zie hieronder)	—	—
2 dec 2027	Volledige AI Act hoog-risico AI-systemen (Bijlage III, was 2 aug 2026)	EU AI Act	Hoog-risico AI-gebruikers
11 dec 2027	CRA volledig van toepassing (conformiteitsbeoordeling)	CRA	Software/hardware-aanb.
2 aug 2028	AI Act: hoog-risico AI ingebed in gereguleerde producten (Bijlage I, was 2 aug 2027)	EU AI Act	Medische/productcombinaties

Geopolitieke Risicocontext — De Storm Achter de Storm

Compliance is niet alleen een juridische verplichting — het is ook een reactie op een veranderend dreigingslandschap. Sinds editie 1 (april 2026) is de geopolitieke context op meerdere fronten verder in beweging gekomen, in twee tegengestelde richtingen tegelijk: verdere escalatie in het Midden-Oosten, en een voorzichtige de-escalatie tussen de VS en Europa.

9.1 Oekraïne — Rusland: onderhandelingen zonder doorbraak

Het gewapend conflict duurt onverminderd voort. Sinds eind 2025 zijn de onderhandelingen tussen Oekraïne, de VS en Rusland concreter geworden — begin augustus 2026 diende Oekraïne een aangepast voorstel in bij de Amerikaanse onderhandelaars — maar een definitief akkoord is er nog niet. Rusland beschuldigt Oekraïne van het torpederen van eerdere afspraken; de strijd, inclusief aanvallen op energie-infrastructuur, houdt aan. De Europese Raad bevestigde in 2026 een steunlening van €90 miljard voor Oekraïne (2026-2027). Voor NL-organisaties blijft de kernboodschap uit editie 1 overeind: nation-state cyberdreiging vanuit Rusland (Sandworm, APT28, Cozy Bear) blijft actueel en NIS2/Cbw-relevant.

9.2 Midden-Oosten: van "conflict" naar oorlog — VS/Israël tegen Iran

Grootste escalatie sinds editie 1: sinds 28 februari 2026 zijn de VS en Israël in een open oorlog met Iran verwickeld (regionaal ook wel de "Derde Golfoorlog" genoemd) — een aanzienlijke opschaling ten opzichte van de meer beperkte spanningen die in editie 1 werden beschreven. Begin augustus 2026 lopen er onderhandelingen (o.a. via Qatar en Oman) over een mogelijk einde van het conflict; president Trump uitte publiekelijk de verwachting dat de oorlog "vrij snel" moet eindigen, maar een akkoord was op het moment van schrijven nog niet gesloten.

Voor Nederlandse organisaties blijven dezelfde compliance-kanalen relevant als in editie 1: energieprijsvolatiliteit en verstoring van scheepvaartroutes (Straat van Hormuz, Rode Zee) raken CER/Wwke-continuïteitsplanning of logistiek/energie-scenario's, en Iraanse statelijke cyberactoren (APT34/OilRig, MuddyWater, APT33) blijven actief tegen Europese kritieke infrastructuur volgens gezamenlijke CISA/NCSC-adviezen.

9.3 USA — Europa: crisis rond Groenland gede-escaleerd, onderliggende spanning blijft

Belangrijke correctie op editie 1: de scherpe confrontatie rond Groenland en Canada die begin 2026 speelde, is in januari 2026 gede-escaleerd. Na dreigementen met invoertarieven (10-25%) en herhaalde uitspraken over Amerikaanse zeggenschap over Groenland, bereikte president Trump tijdens het World Economic Forum in Davos (21-22 januari 2026) een principeakkoord met NAVO-secretaris-generaal Mark Rutte over een "raamwerk" voor toekomstige samenwerking in het Arctisch gebied — waarna de aangekondigde tarieven werden ingetrokken. Denemarken en Groenland benadrukken dat over soevereiniteit niet onderhandeld wordt.

De onderliggende spanning is niet verdwenen: NAVO-functionarissen erkenden medio 2026 dat de intenties van de VS rond Groenland onduidelijk blijven, en het akkoord met Rutte was mondeling, niet schriftelijk vastgelegd. Voor de EU Digital Sovereignty-agenda (Data Act, EUCS, eIDAS 2.0) blijft de episode een aanjager: de kwetsbaarheid van Europese afhankelijkheid van Amerikaanse cloud- en technfrastructuur (95% van EU-cloudcapaciteit bij niet-EU providers) is politiek nog urgenter geworden, ook al is de acute tarievdreiging tijdelijk van tafel.

9.4 USA — China: ongewijzigd sinds editie 1

De technologische ontkoppeling tussen VS en China — halfgeleiderexportcontroles die ASML raken, Huawei/ZTE-uitfasering uit 5G-netwerken, aanhoudende Chinese cyberespionage (Volt Typhoon, APT40) — blijft ongewijzigd ten opzichte van editie 1. Geen nieuwe ontwikkelingen gevonden die de NIS2/CER/CRA-relevantie voor deze dreigingslijn wijzigen.

9.5 Rusland — Europa: hybride dreiging blijft ongewijzigd

Sabotage van kritieke infrastructuur, DDoS-campagnes tegen overheidswebsites en desinformatiecampagnes blijven een structureel dreigingspatroon, ongewijzigd ten opzichte van editie 1. Voor de 11 CER-sectoren blijft dit de meest directe dreigingscontext voor fysieke weerbaarheidsplanning onder de Wwke.

De Stille Storm — IT-Talentschaarste, Genuanceerd

Een belangrijke nuancering ten opzichte van editie 1: de bredere Nederlandse arbeidsmarkt is in de loop van 2026 merkbaar afgekoeld. Waar er in 2024/2025 structureel meer vacatures dan werklozen waren, telde het CBS in het eerste kwartaal van 2026 nog 91 vacatures per 100 werklozen — voor het eerst sinds 2021 minder vacatures dan werklozen. Het totaal aantal openstaande vacatures daalde naar 378.000 (Q1 2026), met een lichte verdere daling in Q2.

Deze afkoeling geldt echter **niet gelijk voor ICT, cybersecurity en AI-rollen**. IT-recruitmentbronnen melden voor 2026 nog altijd 70.000-80.000 openstaande IT-vacatures landelijk, met doorlooptijden van 12-16 weken voor reguliere rollen en 8-12 weken via executive search voor CIO/CISO-posities. UWV en Computable rapporteren dat de schaarste in cloud, cybersecurity, data en AI nog jarenlang zal aanhouden, ondanks productiviteitswinst door AI-tooling. Met andere woorden: de generieke arbeidsmarktkrapte neemt af, maar het senior-specialistentekort dat NIS2/Cbw-, DORA- en AI Act-compliance vereist, blijft structureel.

ENISA schat het EU-brede tekort aan cybersecurityprofessionals nog altijd op circa 500.000; wereldwijd rapporteert de ISC² Cybersecurity Workforce Study een gat van 4,8 miljoen. Deze cijfers zijn niet gecorrigeerd sinds editie 1 in beschikbare bronnen — het beeld van een structureel, meerjarig tekort in precies de rollen die de Perfect Storm vereist, blijft dus staan, ook in een verzachtende bredere arbeidsmarkt.

Vier strategische reacties — ongewijzigd, nu urgenter

- **Geïntegreerde aanpak:** één ISMS (ISO 27001) dekt NIS2/Cbw, DORA, NEN 7510 en BIO2 tegelijk; één AI-governanceframework (ISO 42001) dekt AI Act en AVG-DPIA.
- **Managed compliance services:** vCISO, managed SOC, compliance-as-a-service. €3.000–€8.000/maand tegenover €120K–€160K/jaar voor een inhouse senior CISO.
- **Nearshore/offshore IT-teams:** Polen, Roemenië, Portugal, Noord-Macedonië. AVG-check blijft nodig, ook al is nearshore binnen de EU doorgaans zonder extra doorgifte-problematiek.
- **AI-ondersteunde compliance tooling:** GRC-platforms (ServiceNow GRC, Vanta, Drata, OneTrust) reduceren benodigde mensuren met 30-50% bij gestandaardiseerde frameworks. Tooling vervangt expertise niet.

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. Geen checklist van wat u moet doen, maar de fouten die ik het vaakst zie en die het meeste tijd en geld kosten. Ongewijzigd ten opzichte van editie 1 — met dien verstande dat fout 2, 3 en 6 nu geen theoretisch risico meer beschrijven, maar een lopende verplichting.

1. **Per wet een aparte projectgroep opzetten.** Een ISMS op basis van ISO 27001 is de gemeenschappelijke basis voor NIS2/Cbw, DORA, NEN 7510 en BIO2 tegelijk. Integratie is de hefboom, niet de uitzondering.
2. **Compliance als IT-verantwoordelijkheid behandelen.** Bestuurders die dit volledig delegeren, lopen sinds 15 augustus 2026 persoonlijk, wettelijk risico onder de Cbw.
3. **Meldprocessen per wet apart inregelen.** Vier meldplichten lopen tegelijk bij een ransomware-incident met persoonsgegevens. Eén gecombineerd incidentresponsproces is de enige werkbare aanpak.
4. **AI-tools inzetten zonder governance.** De AI-geletterdheidsplicht geldt al sinds 2 februari 2025, de transparantieplicht sinds 2 augustus 2026.
5. **Leveranciers vertrouwen zonder te toetsen.** DORA art. 28 (sinds jan 2026) en NIS2/Cbw stellen eisen aan uw ICT-toeleveringsketen.
6. **Exit-scenario op papier laten liggen.** De US CLOUD Act heeft dit van juridische formaliteit tot actueel governance-vraagstuk gemaakt.
7. **CRA pas in 2027 op de agenda zetten.** De rapportageverplichting geldt al per 11 september 2026.

Wat wel werkt: vroeg registreren bij NCSC (mijn.ncsc.nl). Sinds 15 augustus 2026 is dit voor circa 8.000 organisaties een verplichting, geen vrijwillige keuze meer — maar registratie geeft ook direct toegang tot dreigingsinformatie en indicatoren.

12

Bronnen & Referenties (selectie — nieuw t.o.v. editie 1)

Editie 1 bevatte 45 geverifieerde bronnen (EU Official Journal, Rijksoverheid, DNB, AP, NCSC, NEN, ENISA, KPMG, IBM, Gartner, McKinsey, CBS, EDPB). Die bronnenlijst blijft grotendeels geldig; onderstaand de kernbronnen die specifiek de wijzigingen in editie 2 onderbouwen.

Onderwerp	Bron
Cbw/Wwke inwerkingtreding 15 aug 2026	NCSC.nl, Rijksoverheid.nl — persbericht 7 juli 2026
AI Act hoog-risico uitstel	Verordening (EU) 2026/1744, PB L, 24 juli 2026 ("Digital Omnibus on AI")
AI Act transparantieplicht 2 aug 2026	Computable.nl, Score Agency — augustus 2026
BIO2 v1.3	bio-overheid.nl, Staatscourant 2026, 7416 n1
Digital Omnibus — kabinetsstandpunt	Kamerbrief staatssecretarissen Aerdts/Van Bruggen, Dutch IT Channel, juni 2026
CRA-guidance Commissie	digital-strategy.ec.europa.eu, C(2026) 5252, 27 juli 2026
GDPR-boetes cumulatief €7,1 mrd	Sectorrapportage 2026 (o.b.v. EDPB-cijfers)
CBS arbeidsmarkt Q1/Q2 2026	CBS.nl — dashboard arbeidsmarkt en vacatures
IT-vacatures 2026	Computable, ICT Recruiter — Q1 2026
Groenland/NAVO-akkoord	Montesquieu Instituut, VRT NWS, Forbes — januari 2026
Iran-oorlog 2026	Al Jazeera, CNN, Britannica — februari t/m augustus 2026
Oekraïne-onderhandelingen	Transport Online, Raad van de EU — augustus 2026

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 databaseveiliging (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, de voor uw sector relevante deadlines en een concrete aanbevelen volgende stap. hes-consultancy.nl/scan — Mike Hes neemt binnen 24 uur contact op voor een vrijblijvend gesprek.

Mike Hes

Oprichter, HES Consultancy International
Calendly: calendly.com/mbhes1970/30min | +31 (0)6 1475 6834

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 **augustus 2026 (editie 2)**. 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