# Beleidskompasformulier voor **internetconsultatie**

**Titel:**

**Cyberbeveiligingsregeling in de Zorg**

## ∞ Wie zijn belanghebbenden en waarom?

Wie zijn direct of indirect belanghebbenden bij het betreffende vraagstuk?

Voor de nationale implementatie van de NIS2-richtlijn in de Cyberbeveiligingswet (hierna: Cbw) is het ministerie van Justitie en Veiligheid (hierna: JenV) het coördinerende ministerie. Vanuit hun rol nemen ze regie op alle ministeriële regelingen. Het ministerie van Volksgezondheid, Welzijn en Sport (hierna: VWS) werkt de sectorspecifieke eisen uit in de Cyberbeveiligingsregeling in de Zorg (hierna: CbrZ)

De directe belanghebbenden zijn de organisaties uit de zorg, entiteiten genaamd in de wet, die onder het toepassingsbereik van de Cbw, het Cyberbeveiligingsbesluit (hierna: Cbb) en daarmee ook onder de ministeriële regeling CbrZ komen te vallen.

De indirecte belanghebbenden zijn de brancheorganisaties en de koepels van het zorgveld. De Inspectie Gezondheidszorg en Jeugd (hierna: IGJ) zal toezicht houden op de naleving van de verplichtingen uit de Cbw, het Cbb en de CbrZ. Het Computer Security Incident Response Team (hierna: CSIRT), te weten Z-CERT, zal ondersteuning leveren aan de entiteiten in de zorg die onder de wet vallen.

- Wie beschikken er over relevante kennis over en ervaring met het vraagstuk?

Onder andere koepelorganisaties, zorgaanbieders, aanbieders van informatietechnologieproducten- of diensten in het zorgveld beschikken over de relevante kennis.

- Op welke wijze zijn belanghebbenden tot nu toe in de verschillende fasen van het beleidstraject betrokken?

Het wetsvoorstel en het besluit zijn eerder in internetconsulatie geweest. Belanghebbende hebben hierop kunnen reageren.

Verder zijn de belanghebbenden betrokken geweest bij de totstandkoming van de regeling middels stakeholderbijeenkomsten met het zorgveld. Tijdens deze bijeenkomsten is het veld op verschillende onderdelen geconsulteerd en geïnformeerd over de voortgang. De IGJ en Z-CERT hebben input kunnen leveren op de regeling.

Vanuit de regierol die JenV heeft, worden via gezamenlijke overleggen de regelingen van alle vakdepartementen besproken en de voortgang bewaakt met oog op inwerkingtreding in Q2 2026.

# 1. Wat is het probleem?

a) Wat is het probleem?

De zogeheten NIS1-richtlijn (Richtlijn (EU) 2016/1148) heeft tot doel het gemeenschappelijke niveau van beveiliging van netwerk- en informatiesystemen in de EU te versterken. De richtlijn biedt de lidstaten bevoegdheid bij de uitvoering van de daarin opgenomen verplichtingen over cyberbeveiliging en het melden van significante incidenten. Deze wetgeving is nationaal geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen (Wbni). Organisaties binnen de sector gezondheidszorg vielen niet onder de reikwijdte van de Wbni. Met de herziening van de NIS1-richtlijn is het zorgveld echter wel als een verplichte sector opgenomen onder de NIS2-richtlijn. Dit betekent dat de vereisten vanuit de NIS2-richtlijn nieuw zijn voor het zorgveld.

Met de implementatie van de Cbw en het Cbb en de bijbehorende sectorspecifieke regeling worden de eisen voor het zorgveld verder uitgewerkt. Daarnaast wordt de IGJ aangewezen als toezichthouder op naleving van de wet voor het zorgveld, en Z-CERT wordt het CSIRT voor het zorgveld in de ondersteuning van significante incidenten.

b) Wat zijn de oorzaken van het probleem?

Met het vaststellen van de NIS2-richtlijn betekent dit dat de wetgeving nationaal wordt geïmplementeerd om de cyberbeveiliging in alle lidstaten te versterken, inclusief de sector zorg. Dit is een hele nieuwe opgave voor de sector zorg, omdat deze geen onderdeel was van de NIS1-richtlijn. Hierdoor krijgt het zorgveld te maken met nieuwe wet- en regelgeving met betrekking tot cyberbeveiliging en de daaruit voortvloeiende vereisten.

c) Wat is de omvang van het probleem?

Zie het antwoord op vraag 1a.

d) Wat is het huidige beleid en wat heeft de evaluatie opgeleverd?

De Europese Commissie heeft de werkbaarheid van de NIS1-richtlijn geëvalueerd en heeft vastgesteld dat de implementatie hiervan in de lidstaten te veel verschilde. Daarom is er gekozen voor een herziening van deze richtlijn. Met deze herziening is de keuze weggenomen dat de lidstaten vrij waren om te kiezen welke sectoren eronder vallen. Het gevolg hiervan is dat het zorgveld nu onder deze wetgeving valt en dus onder het huidige beleid geen vereisten kent met betrekking tot onder andere een zorgplicht en een meldplicht.

Het is niet geheel nieuw voor het zorgveld om cyberveiligheid te hanteren. Het is onder de Wabpvz wettelijk verplicht om aan het normenkader NEN7510 te voldoen. De NEN7510 is een normenkader dat de informatieveiligheid in een organisatie moet waarborgen door de organisaties een kader te bieden waarin ze maatregelen moeten nemen.

e) Wat gebeurt er als de overheid niets doet (Nuloptie)? Wat rechtvaardigt overheidsinterventie?

Nederland is verplicht onder Europese wetgeving om de richtlijnen van de Europese Unie te implementeren. Daarnaast is digitalisering en daarmee de digitale weerbaarheid in alle lidstaten een steeds groter wordend onderwerp. Nederland kan hier niet achterblijven in het verhogen van cyberveiligheid. Met name voor de sector zorg is dit zeker relevant vanwege de grote afhankelijkheid van digitalisering en de wens om digitaal steeds meer uit te wisselen. Hierin is de Cbw cruciaal.

De digitale processen vormen het zenuwstelsel van de Nederlandse maatschappij, en voor vele hiervan zijn wij afhankelijk van buitenlandse, niet-Europese partijen. Zulke digitale afhankelijkheden kunnen risicovol worden als gevolg van geopolitieke ontwikkelingen, met name voor de sector zorg.

# 2. Wat is het beoogde doel?

a) Wat zijn de beleidsdoelen?

Met de implementatie van de Cbw worden algemene eisen gesteld aan de organisaties die onder het toepassingsbereik vallen. Echter, verschillende sectoren vallen onder de wet en moeten aan deze eisen voldoen. Om ervoor te zorgen dat deze eisen duidelijk en toegespitst zijn op de betreffende sectoren, worden deze eisen in de regelingen sectorspecifiek gemaakt. Met de CbrZ worden de eisen die voortvloeien uit onder andere de zorgplicht en meldplicht nader uitgewerkt. Dit omvat het nader uitwerken van de drempelwaarden voor het melden van significante incidenten, het nader uitwerken van de aanwijzing van het CSIRT voor de zorg, en het feit dat de IGJ zal toezien op de naleving van de wet.

De wet en het besluit bieden de ruimte en grondslagen om deze eisen nader te specificeren. VWS maakt hier gebruik van om het veld zo goed mogelijk voor te bereiden op de inwerkingtreding van de wet in Q2 2026.

b) Aan welke duurzame ontwikkelingsdoelen (sustainable development goals, SDG's) en brede welvaartsuitkomsten dragen de doelen bij?

n.v.t.

# 3. Wat zijn opties om het doel te realiseren?

a) Wat zijn kansrijke aangrijpingspunten om het doel te realiseren?

De Cbw, de Cbb en de sectorspecifieke regeling, de CbrZ, resulteren in een wettelijke verankering die aansluit op de doelen die zijn gesteld in de Cybersecuritystrategie 2022-2028 van het NCSC. Het doel wordt bereikt door onder meer plichten op te leggen aan entiteiten, zoals de verplichting tot het treffen van passende en evenredige maatregelen en het melden van significante cyberincidenten. Naast deze plichten zijn er ook rechten voor de entiteiten uit de zorg, zoals het recht op bijstand vanuit de CSIRT (Z-CERT). Dit zijn aangrijpingspunten om de sector zorg als geheel digitaal weerbaarder te maken en om de digitale veerkracht te verhogen. Dit is vooral belangrijk nu er sprake is van toenemende complexiteit in het dreigingsbeeld.

De implementatie van de Cbw en het verhogen van digitale weerbaarheid zullen de basisprincipes vormen om een effectieve barrière te creëren tegen vele verschillende aanvallen vanuit kwaadwillenden in de digitale omgeving.

b) Wat zijn, gegeven de aangrijpingspunten, kansrijke beleidsopties?

Zie 3a.

c) Wat is de beleidstheorie (doelenboom) per kansrijke beleidsoptie?

n.v.t.

# 4. Wat zijn de gevolgen van de opties?

a) Wat zijn de verwachte gevolgen per beleidsoptie?

Met de implementatie van de Cbw en de onderliggende wetgeving wordt het doel bereikt om organisaties te stimuleren tot het verhogen van hun digitale weerbaarheid. Dit heeft als gevolg dat de organisaties die onder het toepassingsbereik van de wet vallen een verhoging in regeldrukeffecten zien. Dit is vanwege de investeringen en inspanningen die gedaan moeten worden om aan de verplichtingen te voldoen, denk hierbij aan o.a. de zorgplicht en de meldplicht.

Daarnaast zullen er toezichts- en handhavingskosten plaatsvinden voor de bevoegde autoriteit in het toezien op de wet, hiervoor zal de IGJ een T&H toets uitvoeren om dit ook voor de regeling verder in kaart te brengen. Verder zullen ook uitvoeringseffecten en -kosten ontstaan voor het CSIRT, dit betekent dat Z-CERT wettelijke taken erbij krijgt voor het bedienen van het zorgveld als CSIRT.

b) Welke verplichte toetsen zijn van toepassing en wat zijn daarvan de uitkomsten (voor zover bekend)?

Er zal een Administratieve lastentoets / regeldrukkosten (Adviescollege Toetsing Regeldruk) worden uitgevoerd.

Er zal ook nog een T&H toets worden uitgevoerd door de IGJ, dit zal gebeuren tijdens de internetconsultatie van de regeling.

# 5. Wat is de voorkeursoptie?

a) Wat is het voorstel?

Voor het traject om de NIS2-richtlijn te implementeren kent deze wet drie lagen: de Cbw, het Cbb en de CbrZ. De wet en het besluit zijn al in een internetconsultatie geweest en bevinden zich in een verder stadium van het proces. Dit werd vanuit de coördinerende rol van het ministerie van JenV begeleid en geregeld. Nu zijn de vakdepartementen aan de beurt om een sectorspecifieke regeling op te stellen die de vereisten uit de wet en het besluit nader uitwerken.

De nader uitgewerkte eisen die in de CbrZ worden opgenomen, moeten worden geconsulteerd met het veld. Hierdoor krijgt het veld de mogelijkheid om input te leveren aan bijvoorbeeld de drempelwaarden voor het melden van een significant cyberincident.

b) Hoe houdt het voorstel rekening met:

- doeltreffendheid en doelmatigheid;
- uitvoerbaarheid voor alle relevante partijen (inclusief doenvermogen, regeldruk en handhaving);

- brede maatschappelijke impact?

Deze regeling betreft een nadere uitwerking van het reeds bij de Tweede Kamer ingediende wetsvoorstel, waarvoor een beleidskompas is ingevuld. De inhoudelijke keuzes die aan de basis van deze regeling liggen, zijn reeds gemaakt in het kader van dat wetsvoorstel. Met de inwerkingtreding van de Cbw, zal deze naar verwachting een stevige impuls geven aan de versterking van de digitale weerbaarheid van Nederland. Dit gebeurt door organisaties, op wie de wet van toepassing is, te verplichten cyberbeveiligingsmaatregelen te treffen en ernstige incidenten te melden.

Dit betekent dat de entiteiten in de zorg hun digitale weerbaarheid op orde moeten hebben, zodat onder meer de patiëntengegevens en het eventuele uitwisselen daarvan op een veilige manier kunnen plaatsvinden. Dit is met name relevant na de maatschappelijke impact die het lek bij Clinical Diagnostics blootstelde en de relevantie van cyberveiligheid binnen organisaties aankaartte.

Bij de uitwerking van deze regeling is rekening gehouden met de regeldruk en de uitvoerbaarheid.

c) Wat zijn de risico's en onzekerheden van dit voorstel?

De onzekerheden van dit voorstel is met name het vraagstuk welke organisaties na inwerkingtreding onder het toepassingsbereik van de wet vallen, en daarmee het recht hebben op bijstand van de CSIRT in het geval van significante incidenten. Welke organisaties onder deze wetgeving vallen is afhankelijk van de grootte en omvang.

d) Hoe ziet de voorgenomen monitoring en evaluatie eruit?

n.v.t.