eOverdracht

# NIS2 en de eOverdracht
# **Informatie voor zorgorganisaties**

**Wat is al bekend en wat kun je alvast doen?**

# Informatie over NIS2 voor zorgorganisaties

## Waarom NIS2?

De Europese informatiebeveiligingsrichtlijn Network en Information Security 2 (NIS2) heeft als doel de digitale veiligheid van systemen en netwerken binnen de Europese Unie te verhogen. De NIS2 is een herziening van de reeds bestaande NIS1 richtlijn, en heeft als doel de weerbaarheid tegen cyberdreigingen verder te versterken. Het toepassingsgebied van de NIS2 is in alle lidstaten gelijkgesteld, waardoor nu ook de sector gezondheidszorg in Nederland onder deze wetgeving valt. Er is een uitzonderingsclausule opgenomen in de NIS2 voor kleine organisaties van minder dan 50 werknemers en/of een omzet van minder dan € 10 miljoen per jaar, de zogenaamde 'size cap'. Dit betekent dat zij buiten het toepassingsgebied van de NIS2[1] vallen. Desalniettemin gelden andere beveiligingsmaatregelen zoals de NEN 7510 wel nog steeds voor deze groep.

## Omzettingsproces

Op Europees niveau is de NIS2 richtlijn op 16 januari 2023 vastgesteld. Momenteel wordt deze Europese tekst omgezet naar nationale wetgeving. Het demissionaire kabinet heeft al laten weten dat de oorspronkelijke implementatiedeadline van 17 oktober 2024 niet zal worden gehaald als gevolg van de complexe implementatie. Er wordt vooralsnog geen nieuwe datum voor de inwerkingtreding genoemd. De internetconsultatie met de concept wetstekst zal vóór de zomer worden opengesteld zodat iedereen kan reageren[2]. De implementatie van de NIS2 in Nederlandse wetgeving is een wet op hoofdlijnen. Hierna volgt de verdere invulling in een Algemene maatregel van Bestuur (AmvB) waarin aanvullende maatregelen worden uitgewerkt. Ook de AmvB zal in internetconsultatie worden opengesteld. Tot slot zal deze AmvB voor de zorg specifiek verder worden uitgewerkt in een ministeriële regeling voor de zorg, met wederom de mogelijkheid tot internetconsultatie. De Nederlandse wetgeving wordt dus stapsgewijs in een kaderwet en lagere wetgeving ingevuld met steeds de mogelijkheid voor het zorgveld om input te leveren.

## Verplichtingen voor zorgorganisaties vanuit NIS2

Omdat het omzettingsproces naar Nederlands recht nog in gang is, is de precieze invulling van de wet afhankelijk van de te maken beleidskeuzes door de verschillende ministeries. Desalniettemin zijn er zes onderdelen van de Europese NIS2-richtlijn die inzicht bieden in de impact die de wet zal hebben.

- **Zorgplicht:** allereerst schrijft de NIS2 een aantal concrete maatregelen voor waaraan zorgorganisaties zich moeten houden (art. 21). Hiermee krijgen zij een zorgplicht en aansprakelijkheid op het gebied van informatiebeveiliging. Echter dekken de reeds verplichte NEN-normen al een deel van deze maatregelen af. Zie hiervoor de mapping in Tabel 1 onderaan deze opsomming.
- **Meldplicht:** ten tweede zullen zorgorganisaties een meldplicht hebben (art. 23). Dit houdt in dat zij verplicht zijn cyberincidenten te melden via het registratie- en meldportaal aan hun Cyber Security Incident Respons Team (CSIRT). Het CSIRT voor de zorg is Z-CERT. Het Nationaal Cyber Security Centrum (NCSC) ontwikkelt een portaal waar Z-CERT op is

[1] Twijfel je nog of je onder de NIS2 valt? Maak dan gebruik van deze zelfevaluatie: NIS 2 Zelfevaluatie NL (regelhulpenvoorbedrijven.nl)
[2] Zodra de conceptwet in internetconsultatie gaat kunt u uw input geven via Overheid.nl | Consultatie, open consultaties (internetconsultatie.nl).

aangesloten. De meldplicht is te vergelijken met de huidige rapportageplicht van persoonsgegevensinbreuken (datalekken) aan de Autoriteit Persoonsgegevens (AP).

- **Informatieplicht:** ten derde hebben zorgorganisaties een informatieplicht (art. 29), wat betekent dat zij relevante dreigingsinformatie over cyberbeveiliging delen via het bovengenoemde portaal. De CSIRTs en de toezichthouders houden zicht op alle meldingen om na te gaan of er een cyberaanval is of anderszins. Zorgorganisaties kunnen in een dergelijk geval een beroep doen op Z-CERT.
- **Toezicht en handhaving:** ten vierde geldt voor zorgorganisaties toezicht en handhaving op de naleving van de NIS2 (art. 32). Dit houdt in dat de onderwerpen waarop de toezichthouder toeziet uitbreiden, en dit toezicht zowel vooraf als achteraf aan incidenten plaatsvindt. Voor de zorgsector zal de Inspectie Gezondheidszorg en Jeugd (IGJ) deze taak vervullen[3]. Daarnaast krijgt de toezichthouder nu handhavingsmaatregelen, zoals gespecificeerd in art. 32. Ook krijgt de toezichthouder de mogelijkheid tot het opleggen van substantiële boetes (art. 34), vergelijkbaar met de boetes die de AP kan uitdelen vanuit de Algemene Verordening Gegevensbescherming (AVG). Voor dit onderdeel is de precieze uitwerking afhankelijk van de invulling in het Nederlands recht.
- **Hoofdelijke aansprakelijkheid:** ten vijfde moeten bestuursleden van zorgorganisaties ervoor zorgen dat zij kennis nemen van de regels uit de NIS2 en dat deze worden nageleefd (art. 20). Zij worden hiervoor zelfs hoofdelijk aansprakelijk. Dit houdt in dat ze voldoende kennis en kunde moeten hebben om de gevolgen van informatiebeveiligingsincidenten in te schatten, en inzicht hebben in de genomen beheersmaatregelen. Hiervoor zullen bestuursleden opleidingen moeten volgen.
- **Bijstand en ondersteuning:** tot slot zullen zorgorganisaties verplichte bijstand en ondersteuning krijgen van een CSIRT (art. 10). Z-CERT is het CSIRT voor de zorgsector. Voor zorgorganisaties die reeds bij Z-CERT zijn aangesloten zullen daarmee geen significante veranderingen plaatsvinden. Zorgorganisaties die niet bij Z-CERT zijn aangesloten kunnen in de toekomst een beroep doen indien zij onder de NIS2 vallen (dus als zij meer dan 50 werknemers hebben en/of een omzet van meer dan € 10 miljoen per jaar).[4]

## Tabel 1: Mapping NIS2 maatregelen (art. 21) op de NEN7510:2017

| NIS2 maatregel | NEN-norm |
|---|---|
| Beleid inzake risicoanalyse en beveiliging van informatiesystemen | NEN 7510-1 H5, H6 en H8 en NEN 7510-2 H5 |
| Incidentenbehandeling | NEN 7510-2 H16 |
| Bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer | NEN 7510-2 H12 en H17 |
| De beveiliging van de toeleveringsketen, met inbegrip van beveiliging gerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners | NEN 7510-1 H4 en NEN 7510-2 H15 |
| Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden | NEN 7510-2 H12, H13, H14, H15 en H16 |
| Beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen | NEN 7510-1 H9 en H10 en NEN 7510-2 H18 |
| Basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging | NEN 7510-1 H7 en NEN 7510-2 H7 en H11 |

[3] Zie voor meer informatie over toezicht ook NIS2-richtlijn | Fysieke en digitale weerbaarheid | Gegevensuitwisseling in de zorg.
[4] Meer informatie over Z-CERT: Wat doet Z-CERT – Z-CERT.

| | |
|---|---|
| Beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie | NEN 7510-2 H10, H13 en H18 |
| Beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa | NEN 7510-1 H7 en NEN 7510-2 H7, H8, H9 en H12 |
| Wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit | NEN 7510-2 H9 |

## Aanbevelingen

Hoewel de precieze uitwerking van de Nederlandse wetgeving nog gaande is, is er al een aantal zaken waarmee je je alvast kunt voorbereiden op de NIS2 wetgeving. Allereerst raden wij je sterk aan om te zorgen dat je voldoet aan de NEN 7510, en in het bijzonder aan de in Tabel 1 genoemde hoofdstukken[5]. Met het voldoen aan deze maatregelen, voldoe je namelijk al deels aan de eisen uit de NIS2!

Daarnaast komen er verschillende rondes van internetconsultatie aan waar iedereen op kan reageren. Hier kun je voorstellen doen over de uitvoerbaarheid en kwaliteit van de conceptwet. Deze consultatierondes bieden bovendien de mogelijkheid om alvast informatie te krijgen over de wet in voorbereiding.

Indien je dit nog niet hebt gedaan, wordt tot slot aangeraden om de CISO en/of IT-afdeling te wijzen op de naderende wetgeving. Zo kunnen zij zich verder voorbereiden op de naderende verplichte maatregelen, meldplicht en informatieplicht.

[5] Download hier de Norm NEN 7510 deel 1 en 2: Norm Detail (webtoolmanagementsystemen.nl).

Samen werken aan eOverdracht