eOverdracht

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

**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 de sector gezondheidszorg ook 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 wet en lagere wetgeving ingevuld met steeds de mogelijkheid 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 tussen de verschillende ministeries. Desalniettemin zijn er een zestal zaken die vanuit de Europese NIS2-richtlijn 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 verplichte meldingen moeten maken cyberincidenten via het registratie- en meldportaal aan hun Cyber Security Incident Respons Team (CSIRT). Het CSIRT voor de zorg is Z-CERT. Het NCSC ontwikkelt een portaal waar Z-CERT op is aangesloten. De meldplicht

[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).

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 uit kan delen 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 van de regels uit de NIS2 kennis nemen en 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. 20 lid 1-2, art. 21 lid 2 en art. 23) op de NEN7510:2024

| Nummer | NIS2 maatregel | Nen7510-1 | NEN7510-2 |
|---|---|---|---|
| 1a | risicoanalysebeleid | 6.1 | |
| 1b | beveiliging informatiesystemen | 6.2 | |
| 2 | incidentafhandeling | | 5.24, 5.25, 5.26, 5.27, 6.8 |
| 3a | bedrijfscontinuiteit | | 5.29 |
| 3b | crisisbeheer | | 5.29, 6.8 |
| 4 | toeleveringsketen | | 6.8 |
| 5a | veilige verwerving | | 8.3 |
| 5b | veilige ontwikkeling | | 8.25, 8.27, 8.31 |
| 5c | veilig onderhoud | | 8.27,8.31,8.32 |
| 5d | kwetsbaarhedenbeheer | | 8.1,8.8,8.19,8.32 |
| 6 | evaluatie beveiligingseffectiviteit | 6.1, 10.1, 10.2 | |
| 7a | zero trust-principes | | 8.35 |

[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.

| | | | |
|---|---|---|---|
| 7b | software-updates | | 8.1, 8.8, 8.15, 8.32 |
| 7c | configuratiebeleid | | 7.9, 7.13, 8.1 |
| 7d | netwerksegmentatie | | 8.22 |
| 7e | identiteitsbeleid | | 5.16 |
| 7f | toegangsbeleid | | 5.18, 8.2 |
| 7g | cybersecuritytraining | | 6.3 |
| 8 | cryptografie | | 8.24 |
| 9a | veilig personeel | | 5.4, 6.1, 6.2, 6.3, 6.4, 6.5 |
| 9b | toegangsbeleid | | 5.15, 5.16, 5.17,5.18,8.2,8.3,8.4,8.5 8.18 |
| 9c | beveiliging van bedrijfsmiddelen | | 5.9, 5.10, 5.11 |
| 10a | MFA/continue authenticatie | | 8.3 |
| 10b | veilige communicatie | | 5.14 |
| 10c | noodcommunicatie | | 5.42 |
| 11 | bestuursgoedkeuring | 5.2, 9.3 | |
| 12 | training bestuursleden | | 6.9 |
| 13 | melden van incidenten | | 5.43 |

## Hoe nu verder?

Hoewel de precieze uitwerking van de Nederlandse Cyberbeveiligingswet nog gaande is, kun je je al wel voorbereiden op deze wetgeving[5]. Begin met voldoen aan de NEN 7510, en in het bijzonder aan de in Tabel 1 genoemde maatregelen[6]. Hiermee voldoe je namelijk al grotendeels aan de eisen uit de NIS2!

Wijs ook uw CISO en/of IT-afdeling op de naderende wetgeving zodat zij zich verder voor kunnen bereiden op de verplichte maatregelen, meldplicht, en informatieplicht.

[5] Voor de laatste stand van zaken, zie Stand van zaken implementatie NIS2 en CER - Digitale Overheid.
[6] Download hier de Norm NEN 7510 deel 1 en 2: https://connect.nen.nl/Family/Detail/69569?compId=16013&collectionId=0 en https://connect.nen.nl/Family/Detail/73550?compId=16013&collectionId=0.

Samen werken aan eOverdracht