STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 28763
14 augustus 2026

Regeling van de Minister van Langdurige Zorg, Jeugd en Sport, van 12 augustus 2026, kenmerk 4494559-1102053-DICIO, houdende regels ter uitvoering van de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit voor de sector Gezondheidszorg en de subsector Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek (Cyberbeveiligingsregeling voor de zorg) [KetenID WGK028136]

De Minister van Langdurige zorg, Jeugd en Sport,

Gelet op de artikelen 20, 24, eerste lid, 27 en 29 van het Cyberbeveiligingsbesluit en artikel 68, eerste lid van de Cyberbeveiligingswet;

Besluit:

HOOFDSTUK 1. ALGEMENE BEPALINGEN

Artikel 1.1 Begripsbepaling

In deze regeling wordt verstaan onder:
– *besluit:* Cyberbeveiligingsbesluit;
– *kritisch bedrijfsproces:* proces dat noodzakelijk is voor de instandhouding van de dienstverlening van een essentiële of belangrijke entiteit;
– *de Minister:* de Minister van Langdurige Zorg, Jeugd en Sport.

Artikel 1.2 Reikwijdte

Deze regeling is van toepassing op de sector Gezondheidszorg en de subsector Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek, bedoeld in bijlage 1 en bijlage 2 van de wet.

HOOFDSTUK 2. NADERE REGELS CYBERBEVEILIGING

Artikel 2.1 Maatregelen

De maatregelen, bedoeld in artikel 21, eerste lid, van de wet en hoofdstuk 4 van het besluit:
a. voldoen aantoonbaar aan het bepaalde in NEN 7510;
b. voldoen aantoonbaar aan het bepaalde de NEN-ISO-IEC 27001 en NEN-ISO-IEC-27002; of
c. hebben aantoonbaar een gelijkwaardig beschermingsniveau.

Artikel 2.2 Criteria significante incidenten

1. Van een significant incident in de zin van artikel 25, tweede lid, onderdeel a van de wet, is sprake indien als gevolg van het incident:
   a. een kritisch bedrijfsproces langer dan vier uur gedeeltelijk of geheel stil ligt;
   b. netwerk- en informatiesystemen die cruciaal zijn voor de instandhouding van de dienstverlening of productie van de belangrijke of essentiële entiteit zijn gecompromitteerd of vernietigd;
   c. de integriteit, vertrouwelijkheid of beschikbaarheid van bedrijfsgevoelige informatie is aangetast;
   d. de vertrouwelijkheid van bijzondere persoonsgegevens of BSN-nummers ten gevolge van een vermoedelijke kwaadwillende handeling zijn aangetast; of
   e. sprake is van blijvend letsel, ziekenhuisopname of overlijden van een persoon.

2. Van een significant incident is tevens sprake indien een incident de gevolgen omschreven in het eerste lid of artikel 25, tweede lid, onderdeel b van de wet kan veroorzaken.

3. Dit artikel is niet van toepassing indien sprake is van voorziene gevolgen van geplande onderhoudswerkzaamheden die door of namens de essentiële entiteit of belangrijke entiteit worden uitgevoerd.

Artikel 2.3 Vroegtijdige waarschuwing

1. In aanvulling op artikel 26, eerste lid, van de wet en artikel 25 van het Cyberbeveiligingsbesluit bevat de vroegtijdige waarschuwing eveneens hoe het incident is ontdekt en de ondersteuning die nodig is vanuit het CSIRT om het incident te beheersen.

2. De in artikel 25, onder b, van het Cyberbeveiligingsbesluit bedoelde gegevens betreffen:
   a. de gevolgen die zijn geïdentificeerd voor het kritisch bedrijfsproces en voor zover bekend bij de leveranciers van de entiteit, die de melding doet en afnemers van producten en diensten van die entiteit; en
   b. de netwerk- en informatiesystemen en vestigingen die zijn geraakt door het incident.

Artikel 2.4 Melding

De gegevens die verstrekt worden bij een melding als bedoeld in artikel 27 van de wet bevatten, voor zover bekend:
a. de oorzaak van het incident;
b. de netwerken en systemen die zijn geraakt door het incident;
c. de gevolgen voor het primaire proces;
d. de gevolgen voor leveranciers aan de entiteit, die de melding doet en afnemers van producten en diensten van die entiteit; en
e. de gevolgen voor de integriteit, beschikbaarheid en vertrouwelijkheid van bijzondere persoonsgegevens, BSN-nummers en bedrijfsgevoelige informatie.

Artikel 2.5 Voortgangs- en eindverslag

Het voortgangsverslag en het eindverslag, bedoeld in artikel 29, eerste en tweede lid, van de wet, omvatten naast de gegevens genoemd in dat artikel, tevens:
a. een beschrijving in hoeverre in de risicoanalyses die voorafgaand aan het incident waren uitgevoerd de in het kader van het incident opgetreden gebeurtenissen waren voorzien, de maatregelen die naar aanleiding van die risicoanalyses zijn genomen en in hoeverre die maatregelen hebben bijgedragen aan beperken van het incident;
b. de wijze waarop het continuïteitsplan is gebruikt en de mate waarin dit plan effectief is gebleken;
c. de betrokkenheid van bij het incident betrokken leveranciers van netwerk- en informatiesystemen, waaronder de:
   1°. afspraken die met deze partijen zijn gemaakt over het voorkomen van cyberincidenten en over het handelen in geval van een cyberincident;
   2°. wijze waarop is gehandeld door de entiteit om het nakomen van deze afspraken te controleren;
   3°. wijze waarop de afspraken door de leverancier van netwerk- en informatiesystemen zijn nagekomen; en
   4°. gezamenlijke evaluatie van het incident; en
d. de lessen die door de entiteit zijn getrokken uit het incident en tot welke maatregelen dit heeft geleid.

HOOFDSTUK 3. AANWIJZING AUTORITEIT EN TOEZICHTHOUDER

Artikel 3.1 Aanwijzingen autoriteit

Als autoriteit als bedoeld in artikel 51, tweede lid, onderdeel i, van de wet, worden aangewezen de ambtenaren van de Inspectie Gezondheidszorg en Jeugd die zijn die belast met het toezicht op de naleving van deze wet voor wat betreft de sector Gezondheidszorg en de subsector Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek, bedoeld in bijlage 1 en bijlage 2 van de wet.

Artikel 3.2 Aanwijzing toezichthouder

Als toezichthouders als bedoeld in artikel 68, eerste lid, van de wet, worden aangewezen de ambtenaren van de Inspectie Gezondheidszorg en Jeugd.

HOOFDSTUK 4. SLOTBEPALINGEN

Artikel 4.1 Inwerkingtreding

Deze regeling treedt in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin zij wordt geplaatst.

Artikel 4.2 Citeertitel

Deze regeling wordt aangehaald als: Cyberbeveiligingsregeling voor de zorg.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

De Minister van Langdurige Zorg, Jeugd en Sport,
W.R.C. Sterk

TOELICHTING

I. Algemeen deel van de toelichting

1. Inleiding

In deze ministeriële regeling wordt de Cyberbeveiligingswet (hierna: Cbw) en het Cyberbeveiligingsbesluit (hierna: Cbb) nader uitgewerkt voor de sector gezondheidszorg en subsector vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek (hierna: subsector vervaardiging). De Cbw en het Cbb stellen sector overstijgende regels en zijn opgesteld in overeenstemming met de betrokken departementen. In deze regeling wordt zoveel als mogelijk aangesloten bij nationale en internationale normen en bestaande processen binnen de zorg. Op deze manier wordt extra regeldruk voorkomen en worden organisaties binnen de zorg geholpen om op een eenduidige manier hun informatiebeveiliging en digitale weerbaarheid te verbeteren.

In deze regeling worden de zorgplicht, meldplicht en drempelwaarden voor significante incidenten uit de Cbw verder uitgewerkt en toegespitst op de sector gezondheidszorg en subsector vervaardiging.

2. Hoofdlijnen van het voorstel

2.1 Algemeen

In de Cbw en het Cbb worden generieke regels gesteld die gelden voor alle sectoren die onder deze wetgeving vallen. In de Cbw en het Cbb zijn delegatiegrondslagen opgenomen om bij een ministeriële regeling nadere regels te stellen over onder meer de zorgplicht, meldplicht en eisen aan het sectorale CSIRT op specifieke beleidsterreinen.

2.2 Doelstelling en noodzaak wetgeving

In deze regeling worden de eisen en verplichtingen die voortvloeien uit respectievelijk de Cbw en het Cbb nader geconcretiseerd. Het doel hierbij is allereerst om de digitale weerbaarheid van de sector gezondheidszorg en subsector vervaardiging te verbeteren. In deze sector en subsector heeft uitval of verstoring van de dienstverlening immers direct invloed op de continuïteit van zorg in onze samenleving. De gezondheidszorg wordt daarnaast steeds meer gedigitaliseerd, wat enerzijds kan leiden tot efficiëntere processen maar anderzijds ook tot toenemende afhankelijkheid van digitalisering en daarmee risico's ten aanzien van informatiebeveiliging. Het digitaliseren en verwerken van medische gegevens vereist een hoog niveau van informatiebeveiliging en digitale veiligheid. Tegelijkertijd is het doel om hierbij zoveel mogelijk aan te sluiten bij de specifieke omstandigheden en behoeften van de sector gezondheidszorg en subsector vervaardigen. Het is van belang om rekening te houden met de regeldruk en administratieve lasten die voortvloeien uit deze regelgeving. Er is daarom voor gekozen om bij de uitwerking van deze regeling zoveel mogelijk aan te sluiten op bestaande sectorale wetgeving en normen. Dit gebeurt bijvoorbeeld door voor de uitwerking van de zorgplicht uit de Cbw aan te sluiten op de (al verplichte) Nederlandse en internationale normen voor informatiebeveiliging, te weten de NEN 7510, en de ISO27001 en ISO 27002.

2.3 Reikwijdte

In de sector gezondheidszorg en de subsector vervaardiging, zoals uitgewerkt in bijlage 1 en bijlage 2 van de Cbw, zijn verschillende categorieën opgenomen waar de entiteiten (op basis van hun grootte en omvang) onder vallen. Deze categorieën zijn dus reeds aangewezen op grond van de Cbw, maar worden voor de volledigheid hieronder nader toegelicht.

Zorgaanbieders

In de NIS2-richtlijn is er voor de definitie van 'zorgaanbieder' aangesloten bij richtlijn 2011/24/EG. Bij de nationale implementatie van de NIS2-richtlijn dient dit begrip verder ingevuld te worden naar de nationale context van de lidstaat. Om aan te sluiten bij de invulling van het begrip 'zorgaanbieder', zoals gehanteerd in de meeste andere sectorale zorgwetten, waaronder de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (hierna: Wabvpz), is ervoor gekozen om in deze regeling de definitie van 'zorgaanbieder' uit artikel 1, eerste lid, van de Wet kwaliteit, klachten en geschillen in de zorg (hierna: Wkkgz) te hanteren. Dat heeft tot gevolg dat entiteiten die niet onder de categorie zorgaanbieder vallen omdat zij bijvoorbeeld alleen jeugdhulp of maatschappelijke ondersteuning aanbieden, niet onder de reikwijdte van de Cbw en daarmee deze regeling vallen.

EU referentielaboratorium

In de NIS2-richtlijn wordt er voor de definitie van 'EU-referentielaboratorium' verwezen naar de Verordening (EU) 2022/2371 inzake ernstige grensoverschrijdende gezondheidsbedreigingen. In deze verordening wordt er onder andere een netwerk van EU-referentielaboratoria voor de volksgezondheid opgericht. Een EU-referentielaboratium is een laboratorium dat door Nederland is aangedragen en door de Europese Commissie is aangewezen om binnen een Europees netwerk samen te werken met andere onderzoeks- en diagnostische instellingen. In het kader van Verordening (EU) 2022/2371 zijn EU-referentielaboratoria verantwoordelijk voor het coördineren van nationale referentielaboratoria op het gebied van volksgezondheid. Taken omvatten het bevorderen van goede praktijken en het aanmoedigen van lidstaten om o.a. diagnose- en testmethoden en melding en rapportage van ziekten op elkaar af te stemmen.

Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren naar geneesmiddelen

Hieronder vallen entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren naar geneesmiddelen zoals gedefinieerd in artikel 1 eerste lid, onderdeel b, van de Geneesmiddelenwet. Hier valt in ieder geval onder entiteiten die (pre)klinisch onderzoek uitvoeren en entiteiten die wetenschappelijk onderzoek met geneesmiddelen uitvoeren zoals bedoeld in artikel 1, eerste lid onderdeel o, van de Wet medisch onderzoek met mensen (hierna: WMO).

Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen vervaardigen

Het betreft in ieder geval entiteiten die onder de Geneesmiddelenwet als de fabrikanten van geneesmiddelen of werkzame stoffen worden aangemerkt zoals bedoeld in artikel 1, eerste lid, onderdeel mm, van de Geneesmiddelenwet. Voor wat betreft farmaceutische bereiding heeft dit betrekking op apotheekbereidingen.

Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek

Het betreft hier entiteiten die medische hulpmiddelen, als bedoeld in artikel 2, onderdeel 1, van Verordening (EU) 2017/745, vervaardigen en entiteiten die medische hulpmiddelen voor in-vitrodiagnostiek, als bedoeld in artikel 2, onderdeel 2, van Verordening (EU) 2017/746, vervaardigen. Deze entiteiten zijn ongeacht de grootte en omvang geclassificeerd als belangrijke entiteiten met uitzondering van gevallen waarin de vervaardigde hulpmiddelen zijn opgenomen op de lijst van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelen.

Entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd ("de lijst van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelen") in de zin van artikel 22 van Verordening (EU) 2022/123

De Commissie kan een noodsituatie op het gebied van de volksgezondheid erkennen overeenkomstig artikel 12, eerste lid, van Besluit nr. 1082/2013/EU. Het Europees Geneesmiddelenbureau (EMA) stelt vervolgens een lijst vast van categorieën kritieke medische hulpmiddelen die zij in het kader van een noodsituatie op het gebied van de volksgezondheid als kritiek beschouwd (artikel 22 van Verordening (EU) 2022/123)). Het gaat hier om entiteiten die medische hulpmiddelen of medische hulpmiddelen voor in-vitrodiagnostiek vervaardigen die op deze lijst zijn opgenomen. Het EMA is onder meer de Europese autoriteit voor paraatheid op gezondheidsnoodsituaties. Aangezien er op dit moment geen noodsituatie is erkend, heeft zij deze lijst nog niet vastgesteld. Zolang er geen noodsituatie is erkend, kunnen er dan ook géén partijen als essentiële entiteit onder deze categorie worden aangemerkt. Wanneer de lijst is vastgesteld worden vervaardigers van kritieke medische hulpmiddelen en kritieke medische hulpmiddelen voor in vitro-diagnostiek aangemerkt als essentiële entiteiten en niet langer als belangrijke entiteiten.

2.3.1 Gemeentelijke Gezondheidsdiensten

Een aantal GGD'en valt zowel onder de sector overheid als onder de sector gezondheidszorg en valt daardoor ook onder twee CSIRT'S (Z-CERT (op dit moment is Z-CERT nog niet aangewezen en acteert het NCSC als CSIRT. Voor verder uitleg wordt verwezen naar paragraaf 3 van deze toelichting) en IBD). Dit leidt tot onnodige dubbele lasten voor deze entiteiten. Daarnaast zijn alle GGD'en reeds aangesloten bij Z-CERT, dat over de benodigde expertise beschikt om hen op een adequate wijze bij te staan in het kader van cyberbeveiliging. Daarom is het passender dat in de samenwerkingsprotocollen, waarin afspraken staan over de samenwerking in de gevallen waarin de CSIRT's overlappende taken hebben, wordt afgesproken dat Z-CERT het voortouw zal nemen bij bijstand aan GGD'en en dat daarbij samengewerkt zal worden met de IBD.

3. Het CSIRT

Sinds de inwerkingtreding van de NIS2-richtlijn heeft Z-CERT enkel taken van CSIRT voor de sector gezondheidszorg en subsector vervaardigen op zich genomen. In afwachting van de formele overlegprocedure met de Algemene Rekenkamer wordt in deze regeling Z-CERT nog niet aangewezen als CSIRT. De Minister van VWS is voornemens om Z-CERT aan te wijzen als CSIRT. Deze aanwijzing zal bij de nabije toekomst alsnog bij regeling plaatsvinden.
Op grond van artikel 2, eerste lid, van het Cbb is de Minister van Justitie en Veiligheid (hierna: JenV) aangewezen als CSIRT. Het Ministerie van VWS heeft met het Ministerie van JenV afspraken gemaakt over de tijdelijke uitvoering van de taken als CSIRT totdat Z-CERT formeel is aangewezen als CSIRT voor de sector gezondheidszorg en subsector vervaardigen. In de periode tussen de inwerkingtreding van deze regeling en de aanwijzing van Z-CERT, kunnen entiteiten die onder de Cbw vallen en recht hebben op ondersteuningen een beroep doen op Z-CERT. Incidenten die in het NCSC-portaal worden gemeld, zullen tevens worden opgepakt door Z-CERT. Voor het uitvoeren van deze werkzaamheden ontvangt Z-CERT reeds subsidie van het Ministerie van VWS.

4. Nadere regels

4.1 Maatregelen

Voor essentiële entiteiten en belangrijke entiteiten als bedoeld in artikel 8 respectievelijk artikel 12 van de Cbw geldt de verplichting om passende en evenredige technische, operationele en organisatorische maatregelen te nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen, die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruiken, te beheersen. Deze verplichting wordt ook wel de zorgplicht genoemd. Artikel 19 van de Cbb biedt de mogelijkheid om de zorgplicht sectoraal nader in te vullen middels een ministeriële regeling van de vakministers voor de sectoren waar zij verantwoordelijk voor zijn.

De maatregelen die essentiële entiteiten en belangrijke entiteiten vallend onder de sector gezondheidszorg of onder de subsector vervaardiging moeten nemen in het kader van de zorgplicht, zijn nader uitgewerkt in artikel 3.1 van de onderhavige regeling.

Een entiteit moet voor de uitvoering van de maatregelen zoals bedoeld in artikel 21, eerste lid, van de Cbw en hoofdstuk 4 van het besluit aantoonbaar voldoen aan hetgeen dat is bepaald in de NEN 7510, of de ISO 27001 en de ISO 27002. Ook kan een entiteit ervoor kiezen om maatregelen te nemen die aantoonbaar een gelijkwaardig beschermingsniveau bieden met het bepaalde in de laatst uitgeven versie van de
NEN 7510, en de ISO 27001 en de ISO 27002. Met 'aantoonbaar' wordt bedoeld, dat een entiteit bewijsmiddelen kan aanleveren waaruit blijkt deze voldoet aan de verplichtingen uit de normenkaders. Het behalen van een certificering toont aan dat een entiteit voldoet aan de norm, maar is in dezen geen vereiste.

Voor zorgaanbieders geldt dat zij op grond van de Wabvpz en het Besluit elektronische gegevensverwerking door zorgaanbieders verplicht zijn om te voldoen aan de beveiligingsvoorschriften zoals vastgelegd in de NEN7510. De NEN7510 is ontworpen voor de zorgsector en sluit aan bij de uitdagingen waar de zorgsector mee te maken heeft. In 2024 is de NEN7510 herzien om beter aan te sluiten bij de eisen die voortvloeien uit de NIS2-richtlijn met betrekking tot de zorgplicht. Deze norm biedt een hoog niveau van informatiebeveiliging ten aanzien van de beveiliging van medische gegevens en, indien relevant, bedrijfsgevoelige gegevens die in de sector gezondheidszorg worden opgeslagen en verwerkt. Om regeldruk te verminderen en dubbele lasten te voorkomen, is ervoor gekozen aan te sluiten bij de NEN 7510. Hiermee wordt nadrukkelijk de keuze gemaakt om aan te sluiten op bestaande en al wettelijk geldende normen.

De verplichting op het voldoen aan de NEN7510 vanuit de Wabvpz is enkel gericht op elektronisch uitwisselingssystemen en zorginformatiesystemen. Het is belangrijk te vermelden dat de zorgplicht in het kader van de Cbw een bredere scope kent. De Cbw gaat expliciet over de beveiliging van alle netwerk- en informatiesystemen die een entiteit gebruikt voor haar werkzaamheden of het verlenen van haar diensten. Anders dan onder de Wabvpz moeten niet alleen uitwisselingssystemen en zorginformatiesystemen voldoen aan de NEN7510, maar moeten ook de andere netwerk- en informatiesystemen, zoals HR-systemen, voldoen aan deze norm.

Zorgaanbieders dienen op grond van de Wabvpz al te werken met de NEN7510. Het ligt dan ook in de lijn der verwachting dat zij deze norm zullen hanteren bij het voldoen aan de verplichtingen die voortvloeien uit de Cbw. NEN7510 bestaat uit twee onderdelen die een samenhangend geheel vormen. NEN7510-1 stelt het normatieve kader vast voor de beheersmaatregelen in de zorgsector. NEN7510-2 geeft uitvoering aan dit kader door de maatregelen toe te lichten, praktische richtlijnen te

formuleren en beste praktijken aan te geven. Deze regeling gaat ervan uit dat beide delen integraal toepassing vinden. Waar in deze regeling naar NEN7510 wordt verwezen, worden zowel NEN7510-1 als NEN7510-2 daaronder begrepen.

Andere entiteiten uit de sector gezondheidszorg en de subsector vervaardiging hoeven niet reeds te voldoen aan de NEN7510. Deze entiteiten kunnen er evenwel voor kiezen om aan deze norm te voldoen. Nu deze norm is toegespitst op de zorg zelf, zal dit niet altijd passend zijn. Deze entiteiten kunnen er daarom ook voor kiezen om de maatregelen die zij dienen te nemen in het kader van hun zorgplicht gelijkwaardig te laten zijn aan het beschermingsniveau van de NEN7510, en de ISO 27001 en de ISO 27002. De bewijslast dat er aan de verplichting wordt voldaan, ligt bij de entiteit.

4.2 Meldplicht

In het Cbb is opgenomen dat er bij ministeriële regeling nadere regels kunnen worden gesteld over artikelen 26 tot en met 30, 33 en 34 van de Cbw. Deze artikelen zien op de meldplicht bij incidenten.

4.2.1 Significante incidenten

In de wet is in artikel 1 opgenomen dat een incident een gebeurtenis is die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt. Een gebeurtenis hoeft niet per definitie plaats te vinden in het cyberdomein. De Cbw kent namelijk een benadering die alle gevaren omvat (*all hazard*) en heeft tot doel om netwerk- en informatiesystemen en de fysieke omgeving daarvan te beschermen tegen gebeurtenissen die de beveiliging van die systemen kunnen aantasten. Het gaat ook om de bescherming van die systemen tegen andersoortige gebeurtenissen, zoals natuurrampen of branden.

Enkel significante incidenten dienen gemeld te worden. Een incident wordt als significant beschouwd wanneer het aan één van de in artikel 3.2 van deze regeling genoemde drempelwaarden of de parameters die in artikel 25, tweede lid, onderdeel b van de wet voldoet of kan gaan voldoen. Onder “kan gaan voldoen” wordt verstaan: “één door een incident veroorzaakte reële kans op de in de drempelwaarden benoemde gevolgen in de (nabije) toekomst waarvan het gevaar op dat moment nog niet is geweken”. Indien een incident potentieel gevaar had kunnen veroorzaken, maar deze door de entiteit binnen 24 uur succesvol is voorkomen of zich feitelijk niet heeft voorgedaan, en er derhalve geen risico meer bestaat dat de gevolgen zoals bedoeld in artikel 3.2 van deze regeling intreden, is sprake van een bijna-incident. Een bijna-incident is niet meldplichtig. Wel kan hiervan op vrijwillige basis melding worden gedaan.

Indien de entiteit in meerdere sectoren valt, dient de entiteit rekening te houden met alle drempelwaarden die voor de verschillende sectoren gelden. Dit betekent dat als één of meer van de drempelwaarden gehaald wordt de entiteit een melding dient te doen.

Geplande onderhoudswerkzaamheden of vooraf overeengekomen onderbrekingen die leiden tot (tijdelijke) onbeschikbaarheid van diensten, worden niet als significante incidenten beschouwd.

4.2.2 Criteria voor significante incidenten in de zorg

Significante cyberincidenten kunnen de dienstverlening van een organisatie of meerdere organisaties aanzienlijk verstoren en hun processen stilleggen. Voor de sector gezondheidszorg en subsector vervaardigen kan dit verstrekkende consequenties met zich mee brengen voor de behandeling van patiënten, de bereikbaarheid en toegankelijkheid van de zorg en het tijdig beschikbaar zijn van geneesmiddelen en medische hulpmiddelen.

De wet bevat algemene parameters, met de mogelijkheid om een of meerdere parameters nader uit te werken met criteria bij ministeriële regeling. Volgens artikel 25, tweede lid, onderdeel a, en onderdeel b, van de Cbw is er sprake van een significant incident als het (a) een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of (b) als het andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Deze ministeriele regeling werkt de meldplicht verder uit middels drempelwaarden specifiek voor de sector gezondheidszorg en subsector vervaardigen. Deze drempelwaarden geven een nadere uitwerking van de wettelijke parameters en beogen entiteiten en toezichthouders duidelijkheid te bieden over wanneer in ieder geval sprake is van een meldplichtig incident.

Met het oog op de uitvoerbaarheid en regeldruk bij entiteiten is ervoor gekozen de parameters die zijn opgenomen in artikel 25, tweede lid, onderdeel b, van de wet niet verder uit te werken in deze regeling. Dit zou immers ertoe leiden dat entiteiten ten aanzien van die criteria specifieke processen

zouden moeten inrichten om tijdig te kunnen vaststellen of zij aan de precies geformuleerde criteria voldoen, zoals een bepaald bedrag aan financieel verlies bij een andere entiteit. Indien een situatie onder de in de regeling vastgelegde drempelwaarden valt, is er sprake van een significant incident dat gemeld dient te worden. Dit sluit echter niet uit dat er in andere gevallen aan de parameter zoals opgenomen in artikel 25, tweede lid, onderdeel b, van de wet kan zijn voldaan en er tevens sprake is van significant incident.

In artikel 3.2, eerste lid, van de regeling is uitputtend geregeld wanneer er wordt voldaan aan de criteria zoals die zijn opgenomen in artikel 25, tweede lid, onderdeel a, van de wet. Indien er aan één of meer van deze drempelwaarden wordt voldaan, dient de entiteit het incident te melden.
De formulering van deze drempelwaarden laat bewust ruimte over voor een entiteit om zelf ten dele invulling te geven aan de drempelwaarden, op basis van de specifieke context en type dienstverlening. Het is bijvoorbeeld aan de entiteit zelf om te specificeren wat in haar situatie verstaan wordt onder kritische bedrijfsprocessen en bedrijfsgevoelige informatie. Dit sluit aan bij de verplichting zoals opgenomen in artikel 16 van het Cbb, voor een entiteit om haar 'assets' te classificeren en hiervan een inventaris te creëren. Om op een adequate wijze risico's te kunnen identificeren die ertoe kunnen leiden dat een belangrijke of essentiële entiteit haar dienstverlening niet meer kan uitvoeren, is het noodzakelijk een duidelijk beeld te hebben van de kritische bedrijfsprocessen. Een organisatie moet daarbij, naast het inventariseren en classificeren van haar assets, bepalen welke processen cruciaal zijn voor het verlenen van de essentiële dienst. Het vaststellen van bedrijfsgevoelige informatie komt terug in de beheersmaatregel 5.12 van de NEN7510-2 om informatie te classificeren op basis het belang voor de organisatie en bijbehorende beschermingsbehoefte.

Hieronder worden de drempelwaarden individueel nader toegelicht. Indien één van deze drempelwaarden wordt overschreden, wordt het incident beschouwd als significant en dient een entiteit altijd melding te doen van het incident. Het is van belang dat een entiteit zelf de afweging maakt of er melding dient te worden gemaakt op basis van de drempelwaarden. Bij twijfel of er wordt voldaan aan één of meer drempelwaarden en het incident wordt niet gemeld, kan het nuttig zijn om de afweging om het incident niet te melden vast te leggen.

a. Een kritisch bedrijfsproces ligt langer dan vier uur gedeeltelijk of geheel stil
   Een incident dat leidt tot een gedeeltelijke of volledige verstoring van het kritisch bedrijfsproces die langer dan vier uur duurt, wordt gezien als significant incident en moet worden gemeld. Met een kritisch bedrijfsproces wordt bedoeld 'een proces dat noodzakelijk is voor de instandhouding van de dienstverlening van een essentiële of belangrijke entiteit'.
   De drempel van vier uur is gekozen omdat dit de minimale periode aangeeft waarin een verstoring merkbare en potentieel ernstige gevolgen krijgt. Deze tijdslijn is ook getoetst met het zorgveld via stakeholdersbijeenkomsten.
   Een verstoring korter dan vier uur kan doorgaans nog worden opgevangen door alternatieve werkprocessen, buffers in de planning, of interne noodmaatregelen. Vanaf vier uur ontstaat echter een situatie waarin geplande behandelingen en diensten niet meer kunnen worden uitgesteld, wachttijden zich opeenhopen en noodmaatregelen niet langer effectief zijn. Een gedeeltelijke of volledige verstoring van een kritisch bedrijfsproces langer dan vier uur vormt daarom een ernstige operationele verstoring van de dienstverlening die rechtstreeks kan leiden tot uitgestelde kritische zorg, beschadiging van medische monsters of therapieën met tijdgebonden werking, en verhoogde fouten door overbelasting van personeel. Dit kan mogelijk ernstige gevolgen hebben voor patiënten.
   Bij een gedeeltelijke of volledige verstoring van het proces moet bijvoorbeeld worden gedacht aan het sluiten van operatiekamers of intensive care afdelingen; het afzeggen van meer dan 20% van de geplande zorg; de uitval van systemen waardoor essentiële informatie voor kritische bedrijfsprocessen niet beschikbaar of betrouwbaar is; het stilleggen van productieprocessen waardoor meer dan 20% van de geplande productie niet kan worden geleverd volgens contractuele afspraken of een verstoring of stillegging van het proces waardoor de veiligheid en kwaliteit van de werking van medische apparaten of hulpmiddelen niet meer kan worden gegarandeerd.
   Onder een gedeeltelijke verstoring wordt verstaan het uitvallen van de noodprocedures, -voorzieningen of -systemen langer dan vier uur. Een gedeeltelijke verstoring kan ook betekenen dat er langer dan vier uur is overgeschakeld op noodprocedures, -voorzieningen of -systemen. In dit geval is de benodigde redundantie van de systemen of processen namelijk onvoldoende gewaarborgd. Gezien de weggevallen redundantie, ontstaat er een reëel risico op ernstige verstoring van de dienstverlening door het incident. Dit moet daarom worden gezien als een significant incident dat de dienstverlening *kan* verstoren.
b. Netwerk- en informatiesystemen die cruciaal zijn voor de instandhouding van de dienstverlening of productie van de belangrijke of essentiële entiteit zijn gecompromitteerd of vernietigd
   Als een incident tot gevolg heeft dat de netwerk- en informatiesystemen die cruciaal zijn voor de instandhouding van de dienstverlening of productie van de entiteit worden gecompromitteerd of vernietigd, dan moet dit gemeld worden.
   Dit betekent dat wanneer netwerk- en informatiesystemen als gevolge van een incident worden

vernietigd of gecompromitteerd, dit naar verwachting een negatief effect heeft op de continuïteit van de dienstverlening. Daarnaast kan de gecompromitteerde of vernietigde netwerk- en informatiesystemen ernstige financiële schade opleveren, wat de financiële solvabiliteit van een organisatie kan aantasten.
Met 'compromitteren' wordt een succesvolle aanval op een netwerk of systeem bedoeld, Dit betekent dat er bij compromitteren altijd te denken is aan onbevoegde toegang waardoor de beschikbaarheid, integriteit en/of vertrouwelijkheid geschaad is, dan wel in gevaar is. Daarnaast is er onder andere te denken aan een offensieve cyberaanval waarbij beademingsapparatuur binnen een ziekenhuis onbruikbaar of onbetrouwbaar wordt. Ook kan hierbij worden gedacht aan gevallen waarbij een onjuiste configuratie van een netwerk- en informatiesysteem het productieproces van een geneesmiddel verstoort waardoor er grootschalige kwaliteitsdefecten ontstaan. In deze gevallen wordt de continuïteit van de dienstverlening van de belangrijke of essentiële entiteit in gevaar gebracht en is het van belang dat een dergelijk incident wordt gemeld.

c. De beschikbaarheid, integriteit of vertrouwelijkheid van bedrijfsgevoelige informatie is aangetast
Het is belangrijk om te melden wanneer de beschikbaarheid, integriteit of vertrouwelijkheid van bedrijfsgevoelige informatie ernstig is aangetast. Onder bedrijfsgevoelige informatie moet in ieder geval worden verstaan die informatie die van belang is voor de beveiliging van de netwerk- en informatie systemen of continuïteit van kritische bedrijfsprocessen en de dienstverlening van een entiteit. Een incident dat de beschikbaarheid, integriteit of vertrouwelijkheid van dit type gevoelige informatie aantast, geeft een grote kans op een operationele verstoring of materiële en immateriële schade.
Onder een aantasting kan men verstaan de aantasting van bedrijfsgeheimen zoals bedoeld in artikel 2, eerste lid, onder a, van de Richtlijn (EU) 2016/943, inclusief de aantasting van intellectueel eigendom dat toekomstige opbrengsten of omzet van de essentiële entiteit of belangrijke entiteit in gevaar brengt. In het geval van een zorgaanbieder kan dit ook patiënt- en cliëntgegevens omvatten, die nodig zijn voor het leveren van zorg.
Een aantasting kan zich ook voordoen wanneer er ongeoorloofd toegang is opgemerkt tot netwerk- en informatiesystemen met bedrijfsgevoelige informatie, en de beschikbaarheid, integriteit of vertrouwelijkheid van de gegevens is aangetast of niet kan worden gegarandeerd.

d. Vertrouwelijkheid van bijzondere persoonsgegevens en BSN-nummers is aangetast ten gevolge van een vermoedelijke kwaadwillende handeling
Als een incident tot gevolg heeft dat de vertrouwelijkheid van bijzondere persoonsgegevens wordt aangetast ten gevolge van een vermoedelijke kwaadwillende handeling, dan is de entiteit verplicht om dit te melden. Met een vermoedelijke kwaadwillende handeling wordt gedoeld op vermoedens van cybercriminaliteit, zoals hacks, diefstal of ransomware-aanval, phishing etcetera. Dat dit ook zo is, hoeft op het moment van melden nog niet vast te staan. Het vermoeden is reeds voldoende om een melding te moeten doen.
In het kader van de Cbw gaat het alleen om digitale gegevens die toegankelijk zijn via netwerk- en informatiesystemen, waarbij de vertrouwelijkheid is aangetast ten gevolg is van een vermoedelijke kwaadwillende handeling.
Significante incidenten waarbij wordt geconstateerd dat er ook sprake is van een inbreuk in verband met persoonsgegevens, dient er mogelijk eveneens gemeld te worden bij de Autoriteit Persoonsgegevens (hierna: AP) op grond artikel 33 van de Algemene Verordening Gegevensbescherming (hierna: AVG). Dit betekent dat een significant incident onder de Cbw waarbij er een inbreuk in verband met persoonsgegevens is in sommige, maar niet alle gevallen, zowel kan worden gezien als een inbreuk in verband met persoonsgegevens onder de AVG als een significant incident onder de Cbw.

e. Sprake is van blijvend letsel, ziekenhuisopname of overlijden van een persoon
Indien een incident bij een entiteit leidt tot blijvend letsel, ziekenhuisopname of overlijden van een persoon, dan is er sprake van een significant incident en dient dit gemeld te worden. Het kan hierbij bijvoorbeeld gaan om een cyberaanval waarbij het proces kortstondig (korter dan vier uur) wordt verstoord, maar waarbij er wel redelijkerwijs te vermoeden is dat er als gevolg van het incident personen zijn overleden. Denk hierbij aan bijvoorbeeld het niet beschikbaar zijn van de juiste patiëntinformatie in een acute situatie of een onvoldoende werking van zorgapparatuur door een incident. In dit geval is er een redelijk vermoeden dat het incident direct in relatie staat tot het overlijden van een persoon.
Het kan hier ook gaan om incidenten waarbij er een onaanvaardbaar risico ontstaat op blijvend letsel, ziekenhuisopname of overlijden van een persoon. Hoewel deze gevolgen nog niet hebben plaatsgevonden, leidt het incident wel tot een reëel risico. Het onaanvaardbare risico op blijvend letsel, ziekenhuisopname of overlijden is enkel meldingswaardig als dit een gevolg is van een verstoring van de netwerk- en informatiesystemen. Er kan sprake zijn van overlap met de meldingsplicht onder de Wkkgz. Hierin is opgenomen dat indien er sprake is van een calamiteit, er een melding gedaan dient te worden bij de IGJ. Er kan hierbij niet worden volstaan met één melding onder de Cbw, aangezien de doelen van beide wetgevingen verschillend zijn.

Totstandkoming drempelwaarden

De IGJ en Z-CERT hebben een adviserende rol vervuld bij het formuleren van deze sectorspecifieke drempelwaarden. Daarnaast is het zorgveld via stakeholdersbijeenkomsten geconsulteerd op eerdere versies van de drempelwaarden. Met deze input zijn de uiteindelijke drempelwaarden opgesteld.

Evaluatie drempelwaarden voor significante incidenten in de zorg

In artikel 24, derde lid, van het besluit is opgenomen dat de doeltreffendheid van de drempelwaarden en de effecten hiervan ten minste elke vier jaar moet worden geëvalueerd door de betrokken vakminister. In deze regeling wordt er afgeweken van deze vier jaar. De criteria die bepalen of er sprake is van een significant incident in de zorg zullen na twee jaar worden geëvalueerd en na de evaluatie zal worden gekeken of deze drempelwaarden gewijzigd dienen te worden of stand houden in de praktijk en werkbaarheid.

4.2.3 Aanvullende informatie bij meldingen

De Cbw en het Cbb bieden de ruimte om aanvullende informatie op te vragen bij de vroegtijdige waarschuwing, melding en het voortgangs- en eindverslag. De aanvullende eisen geven de belangrijke en essentiële entiteiten ook meer richting en duidelijkheid over welke informatie belangrijk is voor zowel het CSIRT als de IGJ in de verschillende fases van het incident. Dit helpt de IGJ en het CSIRT om de ernst en noodzaak van meldingen in te schatten, en de juiste actie te nemen op basis van de ernst van het significante incident. De entiteiten die een melding doen dienen de aanvullende informatie bij de melding in het portaal op te nemen. De keuze om de verdere uitwerking van de melding te specificeren, heeft als doel entiteiten meer handvatten te bieden bij het doen van een melding. Deze uitvraag zorgt voor meer duidelijkheid voor de entiteiten over de informatie die het CSIRT en de IGJ nodig hebben, daarnaast is er rekening gehouden met de fase waarin de melding zich bevindt, om te voorkomen dat entiteiten veel tijd kwijt zijn aan het verzamelen van gegevens, waardoor zij minder adequaat kunnen handelen bij het oplossen van het incident.

Bij de vroegtijdige waarschuwing binnen 24 uur, is er naar verwachting nog onvoldoende bekend over het significante incident. Het voornaamste doel van de melding in deze fase is om de oorzaak en omvang in te schatten en na te gaan waar het CSIRT kan ondersteunen. Deze fase is nodig voor het CSIRT en IGJ om na te gaan over sprake is van een opzichzelfstaand incident of dat er sprake is van een cascade effect.

De melding binnen 72 uur, is voornamelijk bedoeld om zowel de IGJ als het CSIRT een update te geven over het incident. Daarnaast wordt er specifiek gevraagd wat de gevolgen van het incident zijn voor de integriteit, beschikbaarheid en vertrouwelijkheid van bijzondere persoonsgegevens, BSN-nummers en andere bedrijfsgevoelige informatie zoals bedrijfsgeheimen. Indien het incident langer voortduurt dan 72 uur dient er een voortgangsverslag te worden opgesteld, dit zal op verzoek zijn van het CSIRT of de IGJ en zullen in nauw contact blijven met de entiteit over de voortgang.

Bij het eindverslag is het voornaamste doel om te evalueren hoe het incident heeft plaatsgevonden, welke maatregelen wel of niet effectief zijn gebleken en wat er van het significante incident kan worden geleerd. Er wordt daarom onder andere gevraagd om te reflecteren hoe de risicobeoordeling van de entiteit rekening hield met dergelijke scenario's of dreigingen, de effectiviteit van het continuïteitsplan en de rol die de ICT-leveranciers hebben gespeeld bij het significante incident.

Bij de totstandkoming van deze nadere regels over de informatiedeling voor de IGJ en het CSIRT is er rekening gehouden met de bestaande praktijken bij de IGJ en het CSIRT rondom het melden van incidenten en ICT-verstoringen.

5. Toezicht en handhaving

Met het toezicht op de naleving van deze regeling worden ambtenaren van de IGJ belast. Op grond van artikel 68 van de Cbw kan de minister hiervoor ambtenaren bij besluit aanwijzen. De aanwijzing vindt plaats in deze regeling. De betreffende ambtenaren oefenen hun bevoegdheden uit met inachtneming van artikel 69 van de Cbw. Dezelfde ambtenaren die worden aangewezen als toezichthouder, worden met het oog op duidelijkheid voor de praktijk op grond van artikel 3.2 van deze regeling voor de reikwijdte van deze regeling aangewezen als de autoriteit die samenwerkt met de andere autoriteiten, CSIRT's en het centrale contactpunt als bedoeld in artikel 51 van de Cbw.

6. Regeldruk

Inleiding

In de Cbw en het Cbb staan de verplichtingen uitgewerkt die uit deze wetgeving voortvloeien. Voor zowel de wet als het besluit is de regeldruk reeds berekend. In deze regeling worden een aantal zaken specifiek voor de sector zorg nader uitgewerkt. Hoewel naar verwachting de meeste regeldrukeffecten voortvloeien uit de hogere wetgeving, heeft het Ministerie van VWS besloten om aanvullend onderzoek te doen naar de regeldruk specifiek voor de sector gezondheidszorg en subsector vervaardiging. Dit onderzoek is uitgevoerd door een onafhankelijk onderzoeksbureau. Het onderzoek naar de regeldruk van het Cbb en de CbrZ is gecombineerd met het onderzoek naar de regeldruk van het Besluit weerbaarheid kritieke entiteiten (hierna: Bwke) en Regeling weerbaarheid kritieke entiteiten (hierna: Rwkez). De uitkomsten van de regeldruktoets ten aanzien van dit besluit en regeling wordt respectievelijk in die toelichtingen opgenomen.
Het onderzoek heeft betrekking op de verplichtingen die rechtstreeks uit de CrbZ voortvloeien; in het bijzonder de uitwerking van de zorgplicht en de meldplicht. Voor deze verplichtingen is de regeldruk berekend, waarbij onderscheid is gemaakt tussen eenmalige regeldrukkosten en structurele regeldrukkosten.[1] De reden hiervoor is dat enkele bepalingen na het berekenen van de regeldrukkosten zijn gewijzigd of in een later stadium aan de regelgeving zijn toegevoegd. Hierdoor zijn de destijds geraamde regeldrukkosten niet langer representatief voor de huidige situatie.
Bij de herberekening is tevens rekening gehouden met het specifieke perspectief van de zorgsector, aangezien de uitvoering en naleving van de betreffende verplichtingen binnen deze sector tot andere administratieve en organisatorische inspanningen kunnen leiden dan in andere domeinen. De uitkomsten van het onderzoek geven daarmee een actuele en sectorspecifieke weergave van de te verwachten regeldrukkosten.
Via VNO-NCW en MKB-Nederland is getrachteen MKB-toets uit te voeren. Echter was er geen animo en waren er geen deelnemers die bereid waren om te participeren. Om die reden heeft de MKB-toets geen doorgang gevonden.
Voor het berekenen van de regeldrukeffecten is Rijksbreed gehanteerde methodiek voor het kwantificeren van regeldruk, zoals deze staat beschreven in het Handboek Meting Regeldrukkosten 2023.[2]

Aansluiting met de bestaande normen NEN7510 of ISO27001

Middels de CbrZ wordt de zorgplicht zoals deze is opgenomen in de Cbw, en het Cbb, nader uitgewerkt voor organisaties in de zorgsector. Zo wordt bepaald dat deze organisaties aan de zorgplicht kunnen voldoen door naleving van de NEN7510 (versie: 2024), of de ISO27001 (versie: 2022). Voor zorgaanbieders geldt dat zij op grond van de Wabvpz[3], de Wkkgz[4] en het Begz[5] reeds verplicht zijn om te voldoen aan de beveiligingsvoorschriften zoals vastgelegd in de NEN7510.[6] Door aan te sluiten bij deze bestaande en al wettelijk geldende normen wordt gepoogd om de regeldruk van de zorgplicht te verminderen en dubbele lasten te voorkomen. De regelgeving is in het kader nader uitgewerkt.

Eenmalige regeldrukkosten

De eenmalige regeldrukkosten ontstaan voor een belangrijk gedeelte door tijdbesteding voor het uitvoeren van een *gap assessment*, een inventarisatie van de tekortkomingen van de huidige werkwijze ten opzichte van wat wettelijk vereist wordt. Om deze tijdbesteding in te perken maken veel organisaties gebruik van reeds beschikbare ‘mapping’ tussen de NEN7510 en de NIS2, waaronder de versie die beschikbaar is gesteld door het Ministerie van VWS.[NaN] Ook proberen organisaties de regeldrukkosten te verminderen door de taken onderling te verdelen samen met branchegenoten, en door informatiesessies vanuit de brancheorganisatie bij te wonen. Toch verwachten veel organisaties tijd te moeten besteden om een helder beeld te verkrijgen van de extra maatregelen die genomen zullen moeten worden.

Een tweede bron van eenmalige regeldrukkosten zijn eenmalige implementatiekosten. Veel organisaties benadrukken dat hun processen en systemen, in het bijzonder het *Information Security Management System* (ISMS), in grote lijnen al voldoen aan de eisen voortvloeiend uit de zorgplicht. Zij

---

1 Tevens worden de regeldrukkosten van artikel 10, 18 (weren producten en diensten leveranciers), 22 (eisen aan de training), uit de algemene maatregel van bestuur opnieuw berekend. Zodra deze cijfers bekend zijn, zullen deze worden toegevoegd.
2 KCBR, Handboek Meting Regeldrukkosten, 29 november 2023
3 Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
4 Wet kwaliteit, klachten en geschillen zorg
5 Besluit elektronische gegevensverwerking door zorgaanbieders
6 Op basis van onderzoeken van de IGJ (Publicatie IGJ 13-10-2025; Publicatie IGJ 05-06-2025) hebben we aanleiding te denken dat niet alle organisaties volledig voldoen. Echter gaan wij uit van 100% naleving van de huidige wet- en regelgeving (zie hfst. 2.1). https://z-cert.nl/actueel/nieuws/cbweetje-de-nen7510-en-de-zorgplicht

verwachten weinig ingrijpende inhoudelijke wijzigingen van de huidige risicobeheersmaatregelen. De voornaamste tijdbesteding verwachten organisaties van de inspanning om het beleid verder te formaliseren, dat wil zeggen: het ''zwart-op-wit'' vastleggen van deze werkwijzen, en de uitkomsten hiervan.
Op bepaalde thema's stelt de meest recente versie van de NEN7510 en de ISO27001 strengere eisen dan het geval was onder eerdere versies. Een aantal organisaties verwacht daarom eenmalig extra kosten te moeten maken om de werkwijze op het gebied van de beveiliging van de toeleveringsketen aan te passen. Ook de beheersmaatregelen op het vlak van de bedrijfscontinuïteit, en het opstellen van een noodvoorzieningenplan vergen in sommige gevallen een eenmalige additionele tijdbesteding. Gemiddeld genomen schatten de respondenten de eenmalige kosten voor hun organisatie om aan de zorgplicht te voldoen op **€ 45.492** per bedrijf. Deze kosten bestaan voor het overgrote gedeelte uit tijdbestedingskosten voor het (interne) personeel. In onderstaande tabel zijn de totale regeldrukkosten voor de doelgroep weergegeven.

Tabel 4. Eenmalige regeldrukkosten zorgplicht- aansluiting met de NEN7510 en/of ISO27001

Eenmalige of structurele kosten	Kosten per bedrijf (P)	Aantal organisaties (Q)	Totale kosten (P*Q)
Eenmalig	€ 45.492	1.188	€ 54.789.687

Structurele regeldrukkosten

Zoals hierboven benoemd verwacht het gros van de organisaties dat zij hun ISMS slechts op details zullen hoeven aanpassen om het in overeenstemming te brengen met de NEN7510: 2024 en/of de ISO27001: 2022. Toch verwacht een deel van de organisaties structureel extra kosten te zullen moeten maken om deze nieuwe werkwijze uit te voeren. Als belangrijkste oorzaak voor deze kosten wordt de extra tijdbesteding voor de beveiliging van de toeleveringsketen genoemd. Nagenoeg alle organisaties in de sector zorg hebben al staand beleid op dit vlak. m te borgen dat de (directe) leveranciers een vergelijkbaar niveau van beveiliging van de netwerk- en informatiesystemen hanteren als de organisatie zelf, in bijna alle gevallen gevraagd om aan te tonen dat de leverancier gecertificeerd is- of werkt volgens de NEN7510 en/of de ISO27001.
Evenwel verwacht een aantal organisaties dat zij extra tijd zullen moeten besteden aan het controleren van leveranciers, en het opstellen van nieuwe- of openbreken van bestaande leveringsovereenkomsten, om hier clausules in op te nemen op het gebied van de cyberbeveiliging van de leverancier. Gemiddeld genomen verwachten zorgorganisaties dat zij jaarlijks ongeveer één extra Fte nodig zullen hebben om deze taken uit voeren. De corresponderende structurele regeldrukkosten schatten deze organisaties op **€ 55.821** per organisatie. In onderstaande tabel zijn de totale regeldrukkosten voor de doelgroep weergegeven.

Tabel 5. Structurele regeldrukkosten zorgplicht – aansluiting met de NEN7510 en/of ISO27001

Eenmalige of structurele kosten	Kosten per bedrijf (P)	Aantal organisaties (Q)	Totale kosten (P*Q)
Structureel	€ 55.821	1.188	€ 66.314.839

Meldplicht

Organisaties hebben nog geen plicht om melding te doen over cyberincidenten aangezien de wet nog niet van kracht is. Wel geven organisaties aan dat datalekken waarbij persoonsgegevens zijn betrokken op grond van de AVG onder bepaalde voorwaarden moeten worden gemeld bij de Autoriteit Persoonsgegevens. Het verplicht melden van incidenten die uitsluitend van doen hebben met de cyberbeveiliging bij de IGJ én het CSIRT is dus nieuw.

Organisaties hebben veelal een werkwijze ontwikkeld om te melden in het kader van de AVG. Zij verwachten dat cybermeldingen meer impact gaan hebben, niet alleen voor de afhandeling van incidenten maar ook voor het doen van meldingen. Cyberincidenten komen tot op heden weinig voor maar organisaties verwachten dat dit type incidenten meer gaan voorkomen.

Eenmalige regeldrukkosten

Organisaties verwachten beleid te moeten opstellen over hoe incidenten gemeld moeten worden. Dit betreft onder meer wie voor de meldingen binnen organisaties verantwoordelijk zijn, en het opstellen van een werkwijze voor het melden. De schattingen voor de tijd en kosten die hiermee gepaard gaan lopen tussen organisaties uiteen, variërend van eenmaal 5 minuten tot 1FTE gedurende 4 maanden. Gemiddeld zijn de eenmalige kosten per bedrijf **€ 4.162**. De onderstaande tabel geeft de eenmalige regeldrukkosten als gevolg van de meldplicht weer.

Tabel 6. Eenmalige regeldrukkosten meldplicht

Eenmalige of structurele kosten	Kosten per bedrijf (P)	Aantal organisaties (Q)	Totale kosten (P*Q)
Eenmalig	€ 4.162	1.188	€ 4.944.382

Structurele regeldrukkosten

De structurele regeldrukgevolgen bestaan uit het melden van cyberincidenten. Het aantal cyberincidenten die organisaties op jaarbasis verwachten varieert tussen eens in de 10 jaar en 1-2x per jaar. De extra handelingen die organisaties zullen moeten verrichten betreffen het vergaren van gegevens over het incident en het opstellen van verslagen. Organisaties schatten dat dit tussen de 5-10 minuten, oplopend tot enkele dagen, zal kosten. Twee grotere zorgorganisaties verwachten dat zij structureel hogere kosten zullen maken. Ten eerste verwachten zij dat er tot 10 incidenten meldenswaardig zijn per jaar. Eén van de gesproken organisaties is daarom van plan om 1 FTE te besteden aan het afhandelen van meldingen alleen. Een andere organisatie verwacht extra kosten te maken door de verplichting om binnen 24 uur te melden. De gemiddelde structurele kosten per bedrijf worden geschat op **€ 13.875.** De onderstaande tabel toont de structurele regeldrukkosten als gevolg van de meldplicht.

Tabel 7. Structurele regeldrukkosten meldplicht

Eenmalige of structurele kosten	Kosten per bedrijf (P)	Aantal organisaties (Q)	Totale kosten (P*Q)
Structureel	€ 13.875	1.188	€ 13.367.567

7. Financiële gevolgen

Met de inwerkingtreding van de Cbw zullen naar schatting ongeveer 1200 entiteiten binnen de sector gezondheidszorg en sector vervaardiging aan extra verplichtingen moeten voldoen om hun digitale weerbaarheid te verhogen. Het Ministerie van VWS ondersteunt entiteiten door op korte termijn een sectoraal CSIRT voor de zorg aan te wijzen. Het Ministerie van VWS is voornemens om deze rol bij Z-CERT te beleggen. De IGJ zal het toezicht en de handhaving van de Cbw in de gezondheidszorg op zich nemen.

Om de benodigde kennis en capaciteit te waarborgen, heeft VWS de afgelopen jaren geïnvesteerd in de opbouw daarvan. Dit betreft zowel de toekomstige CSIRT-taken van Z-CERT als de toezicht- en handhavingstaken van de IGJ.
Conform de regels van de budgetdiscipline dienen de budgettaire gevolgen te worden ingepast op de begrotingen van de verantwoordelijke departementen. De kosten voor Z-CERT en IGJ worden gedekt vanuit de begroting van het Ministerie van VWS.

8. Advies en consultatie

Een eerdere versie van dit voorstel is voor advies voorgelegd aan het Adviescollege toetsing regeldruk (hierna: ATR), opengesteld voor consultatie op www.internetconsultatie.nl. en voor commentaar toegezonden aan belangenorganisaties en entiteiten. Daarnaast is er een uitvoeringstoets uitgevoerd op deze regeling door de IGJ. Hieronder volgt een globale bespreking van de adviezen, de reacties uit de consultatie en de beoordeling van de uitvoeringstoetsen.
Waar de nummers van de besproken artikelen verschillen, worden de artikelen van die eerdere versie als volgt aangeduid: ([artikelnummer] oud).

8.1 Internetconsultatie

8.1.1 CSIRT[8]

Financiering Z-CERT

Universitaire Medische Centra van Nederland (hierna: UMCNL), Zelfstandige Klinieken Nederland (hierna: ZKN), Nederlandse Vereniging van Ziekenhuizen (hierna: NVZ), InEen en de Nederlandse GGZ vragen om in de regeling te borgen dat Z-CERT meerjarig en structureel wordt bekostigd. Hierop

[8] In de consultatieversie van deze regeling was de aanwijzing van Z-CERT als CSIRT en de bepalingen omtrent de goverance opgenomen. Een aantal reacties zien toe op deze bepalingen. Voor de volledigheid zijn deze opgenomen in deze toelichting en deze reacties zullen, indien aangegeven, worden verwerkt in de regeling waarin Z-CERT wordt aangewezen.

wordt als volgt gereageerd. Z-CERT zal voor het uitvoeren van de wettelijke taken een bekostiging vanuit de begroting ontvangen vanaf 1 januari 2027. Vanaf inwerkingtredingsdatum van de regeling waarin Z-CERT wordt aangewezen als CSIRT tot de start van de bekostiging zal Z-CERT voor de wettelijke taak worden gefinancierd middels de lopende subsidie. Het is niet mogelijk om in de regeling langdurige financiering garanderen. Budgetreservering verloopt conform de Comptabiliteitswet 2016 via de begrotingswetten en niet via lagere regelgeving.

Andere taken Z-CERT

UMCNL wijst erop dat het van belang is dat Z-CERT naast het uitvoeren van de wettelijke taak ook activiteiten kan blijven ondernemen die bijdragen aan het verhogen van de cyberweerbaarheid van de sector. Als reactie hierop wordt verwezen naar de regeling waarmee Z-CERT wordt aangewezen, waarin zal worden opgenomen dat Z-CERT andere activiteiten mag ondernemen zolang deze niet de uitvoering van de wettelijke taak belemmeren of anderszins beïnvloeden.

InEen stelt dat informatieveiligheid niet alleen binnen afzonderlijke eerstelijnsorganisaties, maar juist ook keten breed goed moet zijn geborgd. Om de verbinding binnen die keten te versterken, wordt gevraagd om integrale ondersteuning van zowel zorgaanbieders als hun leveranciers door Z-CERT. Hierop wordt het volgende toegelicht. Organisaties die niet voldoen aan de grootte en omvang van de 'size cap' zullen niet onder de reikwijdte van de wet vallen. Dit zullen veelal de kleinere organisaties met een beperkte capaciteit betreffen. Het feit dat zorgorganisaties niet onder de regeling vallen, ontslaat hen niet van deverplichting om hun netwerk- en informatiebeveiliging op orde te hebben en te voldoen aan de NEN7510. Hoewel het belang wordt begrepen om naast de eerstelijnsorganisaties ook de leveranciers de informatieveiligheid op orde te hebben, is VWS niet voornemens om kleinere partijen financieel te ondersteunen voor hun aansluiting bij Z-CERT. Deze partijen, indien zij niet onder de reikwijdte van de Cbw vallen, zijn zelf verantwoordelijk voor de financiering om deelnemer te worden bij Z-CERT.

8.1.2 Maatregelen

Versienummers

In diverse consultatiereacties, waaronder die van ZKN, de Nederlandse GGZ en ActiZ is geadviseerd om niet te verwijzen naar versienummers van de NEN 7510 en ISO 27001 en ISO 27002, maar om deze te vervangen door 'de op dit moment geldende versie' of woorden van gelijke strekking. Naar aanleiding van deze reactie is artikel 3.1 van de regeling aangepast.

Aantoonbaarheid van de maatregelen

De G4 gemeenten adviseren ons om in artikel 3.1 op te nemen dat er aantoonbaar aan de maatregelen voldaan dient te worden. Dit zal worden toegevoegd aan de bepaling.

NEN7510

In de reacties van UMCNL en Pasquil werd erop gewezen dat de NEN7510, net zoals de ISO 27001, uit een normatief en een niet-normatief deel bestaat. In de reactie wordt tevens ingegaan op de toelichting waarin verwijzingen zijn opgenomen naar het niet-normatieve deel van de NEN7510. Hierop wordt als volgt gereageerd. De NEN7510-1 en NEN7510-2 vormen één geheel: het normatieve kader staat in NEN7510-1 (inclusief de beheersmaatregelen in bijlage A), terwijl NEN 7510-2 deze maatregelen toelicht en richtlijnen biedt voor de implementatie.
Hoewel NEN 7510-2 aanbevelingen bevat, kunnen deze niet zonder meer worden genegeerd. Afwijkingen moeten worden gemotiveerd in de verklaring van toepasselijkheid. NEN 7510-2 geeft daarmee richting aan de *best practices* binnen de zorgsector. Daarnaast sluit deze manier van verwijzen aan bij het Besluit elektronische gegevensverwerking door zorgaanbieders. De verhouding tussen de NEN 7510-1 en NEN 7510-2 zal nader wordt toegelicht in paragraaf 4.1 van de toelichting.

Pasquil wijst erop dat het inventariseren van informatie zoals omschreven in paragraaf 4.2.2 in de toelichting is opgenomen in beheersmaatregel A5.9 NEN7510. Dit punt zal worden overgenomen en de toelichting wordt aangepast.
Pasquil ziet het de eis om assets te classificeren als een aanvullende eis. Dit is namelijk niet verplicht gesteld in de NEN7510. Hierop wordt het volgende toegelicht. Het classificeren van assets is inderdaad geen verplichting die expliciet is opgenomen in de NEN7510, maar het is een verplichting die voortvloeit uit het Cbb. In artikel 15 en 16 Cbb worden eisen gesteld aan beveiligingsaspecten ten aanzien van toegangsbeleid en assets. De beheersmaatregelen die zijn opgenomen in de NEN7510 kunnen hiervoor als richtsnoer worden gebruikt.
Pasquil geeft in haar reactie aan dat niet in de NEN7510 is opgenomen dat het vaststellen van kritische

bedrijfsprocessen een belangrijk onderdeel vormt van de risicobeoordeling.Hierop wordt het volgende toegelicht. Het uitvoeren van een risicobeoordeling is onderdeel van de zorgplicht zoals opgenomen in artikel 21, derde lid, van de Cbw en artikel 7 van de Cbb. In de NEN7510 is niet expliciet opgenomen dat het vaststellen van kritische bedrijfsprocessen een belangrijk onderdeel vormt van de risicobeoordeling. Echter, om op een adequate wijze risico's te kunnen identificeren die ertoe kunnen leiden dat een belangrijke of essentiële entiteit haar dienstverlening niet meer kan uitvoeren, is het noodzakelijk een duidelijk beeld te hebben van de kritische bedrijfsprocessen. In de toelichting zal dit punt nader worden verduidelijkt.

8.1.3 Criteria significante incidenten

Definities

In de consultatie hebben ZKN, Federatie van Medische Technologiebedrijven (hierna: FMed), NVZ en InEen geadviseerd om de term 'incident' te vervangen door de term 'cyberincident' om te voorkomen dat ander soortige incidenten bij het CSIRT gemeld dienen te worden. Hierover wordt het volgende toegelicht. De Cbw kent een benadering die alle gevaren omvat (*all hazard*) en heeft tot doel om netwerk- en informatiesystemen en de fysieke omgeving daarvan te beschermen tegen gebeurtenissen die de beveiliging van die systemen kunnen aantasten. Het gaat hierbij niet alleen om de enkele bescherming tegen gebeurtenissen met kwade wil, zoals digitale aanvallen, diefstal of ongeoorloofde fysieke toegang. Het gaat ook om de bescherming van die systemen tegen andersoortige gebeurtenissen, zoals natuurrampen. Een incident in het kader van de Cbw kan bijvoorbeeld ook een brand in de server ruimte zijn die leidt tot het uitvallen van de netwerk- en informatiesystemen, waardoor de gegevens (deels) niet meer beschikbaar zijn. In de Cbw is de term 'cyberincident' niet opgenomen en in lijn met de wet is deze formulering ook niet opgenomen in deze regeling. In paragaaf 4.2.1 is nader toegelicht wat de wet verstaat onder een 'significant incident'.

ActiZ vraagt om nader te verduidelijken wat er wordt bedoeld met 'netwerk- en informatiesystemen'. Hierop wordt als volgt gereageerd. 'Netwerk- en informatiesystemen' zijn gedefinieerd in artikel 1 van de wet en de regeling sluit aan de definities zoals die zijn opgenomen in de wet.
NVZ, InEen en UMCNL adviseren om de term 'ernstig' te verduidelijken, bijvoorbeeld door artikel 1.1 van de regeling verder aan te vullen. Hierover wordt het volgende toegelicht. In de wettelijke definitie van een significant incident is opgenomen dat het moet gaan om een incident dat ernstige operationele verstoring of aanzienlijke (im)materiële schade veroorzaakt of kan veroorzaken. Deze regeling verduidelijkt wanneer aan deze vereisten is voldaan. Om doublures te voorkomen is daarom gekozen om het woord 'ernstig' in artikel 3.2, eerste lid, onderdeel c en d, van de regeling weg te laten.
UMCNL adviseert om de termen 'gedeeltelijk stilleggen', en 'gecompromitteerd' te verduidelijken en bijvoorbeeld te koppelen aan de impact van bedrijfskritische processen. Er is een verdere verduidelijking van deze termen opgenomen in de toelichting.
UMCNL adviseert om in artikel 3.2, tweede lid van de regeling de reikwijdte van 'kan veroorzaken' nader te duiden zodat onnodig veel meldingen voorkomen worden. De toelichting hierop is als volgt. Hieronder vallen situaties waar er sprake kan zijn van een significant incident indien een incident de gevolgen kan veroorzaken. Hiermee wordt bedoeld een incident die een reële kans heeft op de in de drempelwaarde genoemde gevolgen waarvan het gevaar nog niet is geweken.
Privacy United B.V. wijst erop dat in artikel 25 lid 2 van de Cbw de bewoordingen 'kan treffen' en 'kan veroorzaken' zijn opgenomen. Dit duidt op een bredere scope van het begrip van begrip ' significant incident'. De toelichting hierop is als volgt. In artikel 3.2, tweede lid van de regeling is opgenomen dat er tevens sprake kan zijn van een significant incident indien een incident de gevolgen kan veroorzaken.

De Nederlandse GGZvraagt in hun reactie of onder de drempelwaarde 'netwerk- en informatiesystemen die cruciaal zijn voor de instandhouding van de dienstverlening of productie van de belangrijke of essentiële entiteit zijn gecompromitteerd of vernietigd' ook de gevolgeffecten op het netwerk meenemen wanneer niet-bedrijfskritische toepassingen worden gecompromitteerd. Hierop wordt het volgende toegelicht. Toepassingen die cruciaal zijn voor de instandhouding van de dienstverlening die gecompromitteerd of vernietigd zijn dienen gemeld te worden. Het kan zijn dat het hierbij gaat om een toepassing die in eerste instantie niet als bedrijfskritisch is gedefinieerd. Maar dat deze toepassing wel cruciaal is voor de instandhouding van het netwerk- en informatiesysteem, zal er een melding gemaakt dienen te worden. Welke processen dit zijn, zal moeten blijken uit de risicobeoordeling.

Overlap Wkkgz

De Nederlandse GGZ en NVZ verzoekt om te verduidelijken hoe er wordt omgegaan met de overlap tussen een melding in het kader van de Cbw en de melding die gedaan dient te worden op grond van de Wkkgz. Dit zal nader worden verduidelijkt in paragraaf 4.2.2. van de toelichting.

Artikel 10a MDR

Fmed wijst erop dat de tekst in paragraaf 3.5 onder a niet overeenstemt met hetgeen dat is opgenomen in artikel 10a van de MDR. Hierop wordt de volgende toelichting gegeven. De in de Cbw opgenomen meldplicht staat los van de meldplicht uit hoofde van de verordening Medische Hulpmiddelen (hierna MDR) en de verordening voor In-Vitro Diagnostica (hierna IVDR). Beide verplichtingen hebben een verschillend doel en toepassingsgebied. De meldplicht uit hoofde van de Cbw ziet op significante incidenten die gevolgen kunnen hebben voor de continuïteit of veiligheid van de dienstverlening van essentiële of belangrijke entiteiten. De meldplicht onder de MDR en de IVDR betreft daarentegen het tijdig informeren van bevoegde autoriteiten en zorginstellingen bij (dreigende) leveringsonderbrekingen en strekt ter bescherming van de patiëntveiligheid en de volksgezondheid. Een incident zoals bedoeld in de Cbw leidt niet noodzakelijkerwijs tot een leveringsonderbreking. De toelichting zal naar aanleiding van deze reactie niet worden aangepast.

Bijna-incidenten

Privacy United B.V. vraagt zich af hoe er om moet worden gegaan met 'bijna-incidenten'. Hierop wordt als volgt gereageerd. De meldplicht geldt alleen voor significante incidenten en dus niet voor bijna-incidenten. Entiteiten worden aangemoedigd om een vrijwillige melding te doen in het geval van een bijna-incident.

Passende en evenredige maatregelen

Een organisatie adviseert ons om in artikel 3.1 een tweede lid op te nemen waarin wordt toegevoegd dat maatregelen evenredig moeten zijn in het beheer van de cyberrisico's. Hierop is de volgende reactie geformuleerd. De maatregelen die de entiteit moet nemen, zijn in het kader van artikel 21, eerste lid, van de wet. Daarin is reeds opgenomen dat de passend en evenredig dienen te zijn om de risico's te beheersen.

Aanwezige noodprocedures

ActiZ en UMCNL vraagt om in artikel 3.2 expliciet rekening te houden met de aanwezigheid van noodprocedures die de impact van uitval kunnen beperken. Hierop is de reactie als volgt. Bij elke incident dient de entiteit te toetsen of er wordt voldaan aan de drempelwaarden zoals die zijn opgenomen in de artikel 3.2 van de regeling. Ondanks de aanwezigheid van noodprocedures is het mogelijk dat een gebeurtenis alsnog leidt tot een significant incident, bijvoorbeeld wanneer de netwerk- en informatiesystemen die cruciaal zijn voor de instandhouding van de dienst van de entiteit zijn gecompromitteerd. Daarnaast dient er tevens rekening te worden gehouden met artikel 3.2, tweede lid van de regeling, waarin is opgenomen dat indien een incident de gevolgen zoals omschreven in artikel 3.2, eerste lid, kan veroorzaken, er sprake is van een significant incident.

Fabrikanten gevestigd in het buitenland

Diagned vraagt zich af of het in alle gevallen haalbaar is, dat de in het buitenland gevestigde fabrikant op grond van artikel 26 van de Cbw binnen 24 uur nadat zij kennis heeft genomen van het significante incident een vroegtijdige waarschuwing kan doen. De reactie hierop is als volgt. Een entiteit valt onder de reikwijdte van de Cbw, indien deze in Nederland is gevestigd en diensten verleent of activiteiten verricht in Nederland of een andere lidstaat van de EU. Een fabrikant die buiten Nederland is gevestigd voldoet niet aan het eerste criteria en valt daarmee niet onder de reikwijdte van de Cbw. Mogelijk dienen zij wel een melding te doen op grond van de implementatiewet van de lidstaat waarin de fabrikant is gevestigd.

Aanvullende informatie meldingen

NVZ geeft aan geen bijzondere persoonsgegevens te willen verstrekken bij het doen van een melding bij het CSIRT. Hierop wordt het volgende toegelicht. In zowel de Cbw, als het Cbb als de regeling is niet opgenomen dat er bijzondere persoonsgegevens verstrekt dienen te worden bij het doen van een melding. Bij het doen van een melding in het NCSC portaal zal dan ook niet worden gevraagd naar bijzondere persoonsgegevens.
De NVZ wijst erop dat de verplichting tot het opstellen van een voortgangs- en eindverslag in deze vorm leidt tot een aanzienlijke uitbreiding van de administratieve last. Hier wordt de volgende toelichting op gegeven. Het uitgangspunt is om entiteiten duidelijkheid te bieden over de informatie die de IGJ en het CSIRT nodig hebben bij het in behandeling nemen van een melding en om adequate ondersteuning te bieden dan wel effectief toezicht te kunnen houden. Bij het opstellen van artikel 3.5 van de regeling is aangesloten bij de huidige processen van de IGJ en het CSIRT. Om te voorkomen

dat entiteiten achteraf confronteert worden met de vraag om extra informatie te verstrekken, zijn deze eisen vastgelegd in de regeling.

Meldplicht

ActiZ en de Nederlands GGZ geven aan dat om te kunnen voldoen aan de meldplicht er 24/7 monitoring nodig is. Hierop wordt als volgt gereageerd. In de Cbw is opgenomen dat een entiteit onverwijld of, indien dat niet mogelijk is, binnen 24 uur een vroegtijdige waarschuwing dient te geven en binnen 72 uur een melding dient te doen. Deze termijn begint te lopen op het moment dat de entiteit kennis heeft gekregen van significante incident en niet op het moment dat het significante incident zich manifesteert. De entiteit moet passende en evenredige maatregelen treffen. Het is aan de entiteit om te bepalen of 24/7 passend en evenredig is.
Zowel ZKN als InEen hebben verzocht om één centraal meldpunt te realiseren voor toezichthouders, CSIRTs en de AP, zodat meldingen op grond van de Cbw, de AVG en de Wkkgz slechts eenmaal hoeven te worden ingediend. Naar aanleiding van dit verzoek wordt het volgende toegelicht. Het NCSC beheert het registratie- en meldportaal voor de registraties en meldingen op grond van de Cbw.De AP beschikt over een portaal voor het doen van meldingen in het kader van de AVG. De meldplichten die voortvloeien uit de genoemde wettelijke kaders verschillen in aard en doelstelling, en kennen bovendien ieder een eigen bevoegde instantie, meldstructuur en tijdspad.
VZVZ pleit voor het voorkomen van een dubbele meldplicht als een incident in meerdere sectoren plaatsvindt en te onderzoeken hoe de overlap tussen de toezichthoudende instanties vermeden kan worden en hoe de samenwerking/informatie-uitwisseling tussen deze instanties geborgd worden. Hierop wordt het volgende toegelicht. Vanwege de aard van de richtlijn kan een entiteit in een uitzonderlijk geval onder meerdere sectoren en daarmee ministeriële regelingen vallen. Deze entiteit vallende onder meerdere sectoren krijgt hierdoor meerdere toezichthouders te maken kan krijgen. Deze toezichthouders stemmen onderling hun toezicht af. In de regeling is het niet mogelijk om hier nadere regels over te stellen.
VZVZ merkt op dat de beoordeling of sprake is van een significant cyberincident afhankelijk is van de concrete omstandigheden. Als voorbeeld wordt genoemd dat wanneer binnen de zorg alternatieve systemen beschikbaar zijn, een incident in de praktijk niet altijd zal leiden tot een significante verstoring van de dienstverlening. VZVZ pleit er daarom voor om deze context mee te nemen bij de beoordeling van de impact van incidenten. Naar aanleiding hiervan wordt het volgende opgemerkt. Binnen de Cbw worden significante cyberincidenten niet beoordeeld op basis van de beschikbaarheid van alternatieven of de feitelijke impact op de dienstverlening. De bepalingen zijn erop gericht netwerk- en informatiesystemen te beschermen tegen gebeurtenissen die deze systemen kunnen aantasten. Een incident wordt als significant beschouwd wanneer aan één van de in de Cbw opgenomen drempelwaarden wordt voldaan of kan worden voldaan. De mate van verstoring of de aanwezigheid van alternatieven valt daarmee buiten de reikwijdte van de Cbw. Onder de Wwke wordt daarentegen wel gekeken naar incidenten met een aanzienlijk verstorend effect en kan de beschikbaarheid van alternatieven een rol spelen in de beoordeling. Dit geldt uitsluitend voor entiteiten die als kritiek zijn aangewezen. Om die reden wordt de regeling op dit punt niet aangepast.
ActiZ licht toe dat binnen de VVT-sector veelal wordt gewerkt met SaaS-oplossingen en vraagt of, in het geval van een significant incident bij een dergelijke oplossing, alle zorgorganisaties die daarvan gebruikmaken afzonderlijk een melding moeten doen. Hierop wordt het volgende toegelicht. SaaS-oplossingen, oftewel cloudcomputingdiensten, vallen onder de sector digitale infrastructuur.[9] Voor deze sector geldt de Uitvoeringsverordening (EU) 2024/2690[10], waarin is bepaald wanneer een incident als significant wordt aangemerkt. Deze uitvoeringsverordening is van toepassing op de daarin genoemde entiteiten, zoals aanbieders van cloudcomputingdiensten. Wanneer zich bij een cloudcomputingdienst een incident voordoet, is deze aanbieder verantwoordelijk voor de melding en voor het informeren van rechtstreeks betrokken partijen, zoals o.a. de zorgorganisaties. Een melding is alleen nodig als een leveranciersincident leidt tot een eigen incident dat aan de drempelwaarde voldoet. Zorgorganisaties moeten bovendien contractafspraken met leveranciers maken om de veiligheid van netwerk- en informatiesystemen te waarborgen en deze afspraken controleren.

Drempelwaarden

UMCNL adviseert om artikel 3.2, eerste lid, onderdeel e aan te passen omdat het in de huidige strekking geen causaal verband heeft met het optreden van een incident. Hierop wordt het volgende toegelicht. De drempelwaarde richt zich op incidenten die blijvend letsel, ziekenhuisopname of overlijden van een patiënt kunnen veroorzaken. Dit kan zich voordoen bij onvoldoende patiëntinformatie in acute situaties of onjuiste werking van zorgapparatuur door bijvoorbeeld cyberaanvallen met

[9] De sector digitale infrastructuur valt onder het Ministerie van Economische zaken en klimaat.
[10] Uitvoeringsverordening (EU) 2024/2690 van de Commissie van 17 oktober 2024 tot vaststelling van regels voor de toepassing van Richtlijn (EU) 2022/2555 inzake cyberbeveiligingsrisicobeheer en melding van significante incidenten.

kortdurende verstoringen van processen. Essentieel is echter dat er een direct causaal verband tussen het incident en het schadelijke gevolg bestaat. Een kritieke operatie kan bijvoorbeeld worden uitgesteld door een incident, waardoor de patiënt overlijdt. Ook kan een ambulance niet naar de dichtstbijzijnde Spoedeisende Hulp (SEH) rijden en moet uitwijken naar een ander ziekenhuis, wat resulteert in blijvend letsel of langere ziekenhuisopname. Verder kan informatie over juiste medicatie niet beschikbaar zijn door een incident, waardoor een verkeerde samenstelling wordt gebruikt met gevolgen voor de patiënt.
Daarnaast geeft UMCNL aan dat artikel 3.2, eerste lid, onderdeel a tot en met d afwijkend is ten opzichte van artikel 3.2, eerste lid, onderdeel e. In onderdeel e wordt er over impact op personen geschreven ten opzichte van gevolgen voor bedrijfsprocessen, systemen of gegevens in onderdeel a tot en met onderdeel d. UMCNL vraagt of deze elementen voldoende in evenwicht zijn. Hier wordt het volgende op toegelicht. De in onderdeel a tot en met d genoemde drempelwaarde zijn toepasbaar op een bredere scala aan gevolgen met betrekking tot bedrijfsprocessen en netwerk- en informatiesystemen. De drempelwaarde onder onderdeel e geeft een extra risico aan ten opzichte van een significant incident, dit zal niet altijd gelijk meetbaar zijn ten opzichte van de drempelwaarde onder a tot en met d. Het doel van de Cbw is de continuïteit te waarborgen en netwerk- en informatiesystemen te beschermen, het is vanzelfsprekend dat er meerdere drempelwaarden zijn gericht op bedrijfsprocessen, systemen, etcetera.De drempelwaarden zijn in evenwicht, omdat de scenario's genoemd onder a tot en met d in een worst-case scenario ook gevolgen kunnen hebben die doorwerken in de drempelwaarde onder e. Dit betekent dat ernstige verstoringen van bedrijfsprocessen, netwerk- en informatiesystemen of gegevensverlies uiteindelijk kunnen leiden tot impact op personen of patiënten.
Verder geeft UMCNL aan dat het passend zou zijn als onder de uitzondering van artikel 3.2 derde lid van de regeling ook wordt opgenomen dat uitval of een incident zoals een defect, brand, waterschade, leveranciersprobleem of een menselijke fout uitgezonderd zijn van de meldplicht indien met voldoende zekerheid kan worden vastgesteld dat deze niet gerelateerd zijn aan een significant incident. UMCNL verwacht dat er anders veel niet-relevante meldingen zullen gemaakt worden als deze uitzondering niet wordt opgenomen. Hierop wordt het volgende toegelicht. De Cbw volgt een all-hazard benadering, die alle gevaren omvat, en tot doel heeft om netwerk- en informatiesystemen en de fysieke omgeving daarvan te beschermen tegen gebeurtenissen die de beveiliging van die systemen kunnen aantasten. Dit omvat niet alleen de bescherming tegen gebeurtenissen met kwade wil, zoals digitale aanvallen, diefstal of ongeoorloofde fysieke toegang, maar ook bescherming tegen andersoortige gebeurtenissen, zoals natuurrampen. De voorbeelden die UMCNL aanhaalt, zijn gebeurtenissen die kunnen leiden tot een significant incident als de gevolgen die in artikel 3.2, eerste lid zijn opgenomen. Indien dat niet het geval, is er geen sprake van een significant incident en hoeft de belangrijke of essentiële entiteit geen melding te doen. Daarnaast dient er rekening te worden gehouden met artikel 3.2, tweede lid waarin is opgenomen dat er tevens sprake is van een significant incident indien het incident de gevolgen in artikel 3.2, eerste lid kan veroorzaken.
Pasquil merkt op dat artikel 3.2, eerste lid, onderdeel a, teveel ruimte laat aan de entiteit om zelf te bepalen wat als een kritisch bedrijfsproces wordt beschouwd. Daarbij wordt aangegeven dat het onderscheid tussen acute en niet-acute zorg niet duidelijk is omschreven en dat het wenselijk zou zijn ruimte te bieden voor verschillende tijds- of impactcriteria per type zorgproces. Hierop wordt het volgende toegelicht. Het is aan de entiteit zelf om vast te stellen wat onder een kritisch bedrijfsproces valt, deze kunnen worden geïdentificeerd aan de hand van de in deze regeling gedefinieerde definitie. Gezien de diversiteit aan typen zorgprocessen binnen de sector is het niet mogelijk deze definitie verder te preciseren zonder af te doen aan de noodzakelijke uitvoeringsruimte voor de verschillende zorgaanbieders.
Daarnaast merkt Pasquil op dat artikel 3.2, eerste lid, onderdeel c, waarin wordt verwezen naar "bedrijfsgevoelige informatie", als een aparte drempel wordt gepresenteerd. Volgens Pasquil is niet duidelijk wat dit toevoegt aan de criteria rond kritische bedrijfsprocessen en lijkt deze extra benoeming overbodig. Hierop wordt het volgende toegelicht. Een incident kan aan meerdere drempelwaarden voldoen. De drempelwaarde betreffende bedrijfsgevoelige informatie is opgenomen omdat het uitlekken van informatie niet noodzakelijkerwijs leidt tot het stilvallen van een kritisch bedrijfsproces, maar wel tot een verstoring van de dienstverlening.
Ten aanzien van artikel 3.2, eerste lid, onderdeel d, wordt verzocht om eenduidigheid bij de verwijzing naar persoonsgegevens. Pasquil stelt dat het BSN een persoonsgegeven is en betoogt dat het onoverzichtelijk is om BSN slechts als voorbeeld van (bijzondere) persoonsgegevens te behandelen. Hierop wordt het volgende toegelicht. In deze drempelwaarde wordt expliciet verwezen naar bijzondere persoonsgegevens en niet alle persoonsgegevens. De BSN nummers zijn geen bijzonder persoonsgegevens en worden daarom expliciet benoemd in de drempelwaarde.
Bij artikel 3.2, tweede lid, wordt verzocht de meldplicht uit te breiden naar "events" die zouden kunnen uitgroeien tot significante incidenten, en te verduidelijken dat reguliere verstoringen niet onder de meldplicht vallen. Hierop wordt het volgende toegelicht. In artikel 3.2, tweede lid, is opgenomen dat een incident gemeld dient te worden als er een reële kans is op het kunnen veroorzaken van een significant incident. Dit betekent: een door een incident veroorzaakte reële kans op de in de drempelwaarden genoemde gevolgen in de (nabije) toekomst, waarbij het gevaar op dat moment nog niet is geweken. Daarnaast is er in artikel 3.2, derde lid opgenomen dat geplande onderhoudswerkzaamhe-

den of vooraf overeengekomen onderbrekingen, die leiden tot (tijdelijke) onbeschikbaarheid van diensten, geen significante incidenten zijn. Reguliere verstoringen vallen hieronder. Om deze reden wordt de uitbreiding niet meegenomen in deze regeling.
De NVZ geeft in haar reactie aan dat er duidelijke minimale grenswaarden moeten worden vastgesteld voor wanneer sprake is van een significant incident. De reactie hierop is als volgt. Volgens de wet is een incident significant als het (i) een ernstige operationele verstoring van diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken, of (ii) andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Deze wettelijke drempelwaarden bieden een brede omschrijving van wat als een significant incident wordt beschouwd. In de regeling wordt daarom nadere invulling gegeven aan de zorgspecifieke drempelwaarden. De wettelijke drempelwaarden vormen daarmee de minimale grens voor het vaststellen van een significant incident.
Diagned, mede namens Nefemed en FME Zorg, vraagt zich af of voor de hulpmiddelensector voldoende duidelijk is gedefinieerd wanneer sprake is van gedeeltelijke of volledige verstoring van een kritisch bedrijfsproces die langer duurt dan 4 uur. De in de toelichting genoemde voorbeelden roepen vragen op. Het verzoek vanuit Diagned is om de regeling, en in ieder geval de toelichting, zodanig aan te passen dat deze ook goed uitvoerbaar is. Hierop wordt het volgende toegelicht.
Entiteiten die in Nederland gevestigd zijn en diensten verlenen of activiteiten verrichten in Nederland of een andere lidstaat van de EU, dienen een significant incident te melden als dit aan de drempelwaarden voldoet. Voor de belangrijke en essentiële entiteiten geldt dat de precieze invulling van deze drempelwaarden kan verschillen, afhankelijk van hun kritische bedrijfsprocessen en cruciale netwerk- en informatiesystemen. Bij het opstellen van de drempelwaarde is zoveel mogelijk rekening gehouden met de verschillende sectoren en hun processen. Gezien de grote diversiteit binnen de sectoren die onder deze regeling vallen was het echter niet mogelijk om expliciet per (sub)sector een drempelwaarde te stellen. De genoemde voorbeelden in de toelichting bieden een leidraad, maar het is aan de entiteit zelf om bijvoorbeeld te bepalen welke bedrijfsprocessen kritiek zijn en niet langer dan 4 uur stil mogen liggen, of welke netwerk- en informatiesystemen cruciaal zijn.
Sensire geeft aan dat het onduidelijk is over wie er moet melden indien er bijvoorbeeld bij een leverancier een storing optreedt die invloed heeft op de zorginstellingen. Daarnaast geeft Sensire aan dat artikel 3.2 meer praktische handvaten nodig heeft. Het uitwerken van scenario's zal meer duidelijkheid scheppen wanneer er gemeld dient te worden. Hierop wordt het volgende toegelicht. In de Cbw en het Cbb is er geen delegatiegrondslag opgenomen om nadere regels te stellen over de uitvoering van de meldplicht, anders dan welke informatie de entiteit dient te verstrekken bij het doen van melding. Er zal worden onderzocht hoe hier via een andere weg invulling kan worden gegeven aan dit advies.
Een organisatie geeft aan dat artikel 3.2 eerste lid, onderdeel d kan leiden tot veel onduidelijkheid. Er wordt aangegeven dat potentieel alle meldingen over gezondheidsgegevens die aan de AP gedaan moeten worden onder deze drempelwaarde vallen, maar lijkt dat qua aard en omvang niet passend bij de andere criteria. Het voorstel vanuit deze organisatie luidt om naast de ernst ook de omvang van de gegevens te specificeren. De reactie hierop is als volgt. In het kader van de Cbw betreft het alleen de digitale gegevens die toegankelijk zijn via netwerk- en informatiesystemen. In de toelichting wordt het melden van een incident aangeduid met een vermoedelijke kwaadwillende handeling. Incidenten waarbij geconstateerd wordt dat er een inbreuk is gemaakt op persoonsgegevens dienen mogelijk eveneens gemeld te worden bij de AP. Er kan zich een situatie voordoen waar zowel een melding op grond van de Cbw als een melding op grond van de AVG gedaan dient te worden.

8.1.4 Reikwijdte

VZVZ pleit ervoor om als organisatie onder de meldplicht van de sector gezondheidszorg te vallen, in plaats van onder de sector digitale dienstverlening, waar ze onder komen te vallen. VZVZ argumenteert dat hierdoor de meldingen niet bij de toezichthouder van de sector zorg vallen, maar bij een andere toezichthouder. Dit terwijl VZVZ zich richt op de sector zorg, en verschillende diensten aanbiedt. Hierop wordt het volgende toegelicht. De Cbw biedt niet de mogelijkheid om een entiteit aan te wijzen onder een andere sector. VZVZ is, gezien de werkzaamheden, een digitale dienstverlener en valt daarom van rechtswege onder de sector digitale dienstverlening.
NVZ geeft aan dat alle leveranciers van ICT-systemen die worden ingezet voor het primaire zorgproces onder het toezicht van de IGJ zouden moeten vallen. Hierop wordt het volgende toegelicht. Leveranciers van ICT-systemen die voldoen aan de grootte en omvang van de sector digitale infrastructuur, zullen onder deze sector vallen. Zij dienen zich te registeren bij het Nationaal Cyber Security Centrum (NCSC). Meldingen van significante incidenten dienen tevens gedaan te worden bij het NCSC. Daarnaast vallen deze entiteiten onder het toezichtregime van de Rijksdienst voor Informatie en Communicatie (RDI). Als deze systemen primair worden ingezet voor het primaire zorgproces, is het aan de toezichthouders om onderling samenwerkingsafspraken te maken. Dit om onder andere informatie uit te wisselen en zo de veiligheid en integriteit van de ICT-systemen in de zorgsector te waarborgen.
Een organisatie vraagt om duidelijkheid omtrent de verplichtingen, de verantwoordelijkheid en

uitvoeringslasten waar de GGD'en mee te maken krijgen. Hierop wordt het volgende toegelicht. GGD'en zijn zorgaanbieders en vallen in die hoedanigheid onder de sector gezondheidszorg. De GGD'en die rechtstreeks onder de gemeente vallen, maken daarnaast ook deel uit van de sector overheid. Met het Ministerie van BZK is afgestemd dat het passender is dat in de samenwerkingsprotocollen, waarin afspraken staan over de samenwerking in de gevallen waarin de CSIRT's overlappende taken hebben, wordt afgesproken dat Z-CERT het voortouw zal nemen bij bijstand aan GGD'en en dat daarbij samengewerkt zal worden met de Informatie Beveiligingsdienst die als CSIRT voor de sector overheid zal fungeren. De toelichting zal naar aanleiding hiervan worden aangevuld.

8.1.5 Overig

Financiële ondersteuning

ZKN vraagt of het ministerie onderzoek kan doen naar de mogelijkheden om zorgaanbieders buiten de reikwijdte financieel te ondersteunen bij de aansluiting bij het CSIRT. Hierop wordt het volgende toegelicht. Het financieel ondersteunen bij de aansluiting bij het CSIRT betreft een IZA-afspraak waarin dit is opgenomen. Op een later moment is gecommuniceerd dat het Ministerie van VWS niet voornemens is om de verdere aansluiting te financieren. De verantwoordelijkheid ligt bij de partijen, die niet onder de reikwijdte van de Cbw vallen, zelf om de aansluiting te financieren, indien er behoefte is om gebruik te maken van de diensten van het CSIRT.

Cyberbeveiligingsbesluit

NVZ en de Nederlandse GGZ hebben een reactie opgesteld met de vraag voor nadere uitwerking van artikel 18 Cbb in de regeling om daarin de patiëntveiligheid mee te nemen bij het toepassen van deze vorm van ingrijpen. Hierop wordt het volgende toegelicht. Indien er gebruik wordt gemaakt van dit artikel, wat alleen als 'last resort' wordt ingezet, maakt de minister een integrale afweging waarin dergelijke punten zullen worden meegenomen indien de minister dit nodig acht.

Sensire verzoekt in haar reactie om meer duidelijkheid over de verplichtingen die voortvloeien uit artikel 10, tweede lid, van de Cbb. Vanuit het oogpunt van effectiviteit en het beperken van administratieve lasten vraagt Sensire het Ministerie van VWS richting te geven aan de wijze waarop het toezicht op IT-dienstverleners en zorginstellingen wordt vormgegeven, bij voorkeur door dit te centraliseren bij de toezichthouder. Daarop wordt het volgende toegelicht. De Cbb legt deze verplichting nadrukkelijk bij de partijen zelf. Zij weten immers van welke toeleveranciers zij gebruikmaken en welke contractuele afspraken daarbij gelden. Het vaststellen van beleid behoort niet tot de taken van de toezichthouder; deze beoordeelt uitsluitend of organisaties aantoonbaar beleid hebben vastgesteld.

Ketenverantwoordelijkheid

BVKZ uit haar zorgen over de verplichting voor leveranciers om te voldoen aan de zorgplicht, zoals omschreven in artikel 3.1 van de regeling. Voor kleine zorgaanbieders die optreden als leverancier van een essentiële of belangrijke entiteit brengt dit extra kosten en regeldruk met zich mee. Daarnaast pleit BVKZ voor een verduidelijking van het begrip *toeleverancier*, waarbij wordt aangegeven aan welke voorwaarden kleinschalige zorgaanbieders moeten voldoen. Hierop wordt als volgt gereageerd. De verplichting tot het beveiligen van de toeleveringsketen ziet uitsluitend op aspecten van de toeleveringsketen die relevant zijn voor de beveiliging van de netwerk- en informatiesystemen die de entiteit gebruikt voor haar werkzaamheden of die zij voor het verlenen van haar diensten gebruikt. Een kleine zorgaanbieder zal doorgaans niet worden aangemerkt als toeleverancier, aangezien de diensten die deze levert niet relevant zijn voor het de beveiliging van de netwerk- en informatiesystemen van de belangrijke of essentiële entiteit.
BVKZ pleit ervoor dat kleine zorgaanbieders zich primair richten op het voldoen aan de basisvereisten en hun softwareleveranciers en externe ICT-partijen vragen om aantoonbare certificering volgens NEN 7510 of ISO 27001. Zij kunnen daarbij aansluiten bij de vijf basisprincipes van digitale weerbaarheid van het NCSC, die als referentiekader dienen voor kleinschalige zorgaanbieders. BVKZ vraagt daarnaast aandacht voor hun positie: door hun beperkte omvang beschikken zij vaak niet over een eigen ICT-afdeling en hebben zij behoefte aan concrete handvatten om aan wet- en regelgeving te voldoen. Hierop wordt het volgende toegelicht. Organisaties met minder dan 50 fte of een jaaromzet en balanstotaal van minder dan 10 miljoen euro vallen buiten de reikwijdte van de Cyberbeveiligingswet. Hoewel het belang wordt onderschreven van goede naleving en een goede informatieveiligheid, zijn zij niet verplicht te voldoen aan de Cbw. Kleinschalige zorgaanbieders zijn echter al op grond van de Wabvpz verplicht te voldoen aan NEN 7510 en dragen daarmee actief bij aan hun informatieveiligheid.

8.2 Advies Adviescollege toetsing regeldruk

Het ATR adviseert toe te lichten hoe bij de uitwerking van de zorgplicht de samenhang met andere sectorspecifieke regelingen is geborgd en hoe dubbele (toezichts)lasten worden voorkomen. Hierop wordt het volgende toegelicht. De aard van de richtlijn brengt met zich mee dat het onvermijdelijk is dat in een enkel geval een entiteit onder meerdere sectoren valt en daarmee onder meerdere ministeriele regelingen. Zij krijgen in dat geval te maken met meerdere toezichthouders en meerdere CSIRTs. De toezichthouders stemmen onderling af hoe zij het toezicht gaan vormgeven en hoe zij omgaan met toezicht op entiteiten die te maken hebben meerdere toezichthouders. Ook tussen de CSIRT's zullen onderling afspraken worden gemaakt. Voorzover mogelijk is er rekening gehouden met de samenhang tussen de andere sectorspecifieke regelingen, bijvoorbeeld ten aanzien van de zorgplicht. Op dit moment is er geen aanleiding om de regeling aan te passen.
Het ATR adviseert nader toe te lichten hoe risicogericht en proportioneel toezicht vormgegeven wordt en op welke wijze stapeling van toezicht wordt voorkomen. De reactie hierop is als volgt. Het uitgangspunt van de toezichthouder is om risicogestuurd en proportioneel toezicht te houden. Dit wordt verder vormgegeven door de toezichthouders. In de wet of het besluit is er geen delegatiegrondslag opgenomen voor het stellen van nadere regels in de ministeriële regeling over dit specifieke punt.
Het ATR adviseert te onderbouwen hoe de drempelwaarden tot stand zijn gekomen en welke mogelijk minder belastende alternatieven zijn overwogen. Naar aanleiding van dit advies is de toelichting op verschillende punten aangevuld en verduidelijkt.
Het ATR adviseert te onderbouwen hoe onnodige stapeling van meldingen worden voorkomen en ten behoeve hiervan één centraal (waar nodig ook binnen Europees verband) meldpunt te faciliteren. Hierop wordt het volgende toegelicht. Significante incidenten dienen gemeld te worden in het NCSC-portaal. Hier worden alle meldingen verzameld en vervolgens doorgezet naar de betrokken toezichthouder(s) en CSIRT(s). Indien er sprake is van een grensoverschrijdend component zal het NCSC deze, als nationaal CSIRT, delen met de andere lidstaten. Het kan voorkomen dat er tevens een melding moet worden gedaan bij de AP indien er sprake is van een inbreuk in verband met persoonsgegevens. Dit zijn twee afzonderlijke meldingen onder twee verschillende regimes. In de wet of het besluit is er geen delegatiegrondslag opgenomen voor het stellen van nadere regels in de ministeriële regeling over het meldportaal.
Het ATR adviseert nader te onderbouwen waarom de regeling een nationale kop zet op de rapportageverplichtingen voor zorgorganisaties. Naar aanleiding van dit advies is de toelichting aangevuld met een verdere onderbouwing.
Het ATR adviseert toe te lichten of aan de noodzakelijke randvoorwaarde van voldoende gekwalificeerd personeel in de zorg is voldaan. Hierop wordt als volgt gereageerd. Gezien de arbeidstekorten in de zorg, met name bij functies die kennis van de IT-sector vereisen, wordt zo veel mogelijk aangesloten bij bestaande normenkaders zoals de NEN 7570 en ISO 27001/27002.
Het ATR adviseert bij de zorgplicht met betrekking tot de beveiliging van de toeleveringsketen aan te geven hoe (kleinere) zorgorganisaties bij deze verplichting worden ondersteund. Hierop wordt als volgt gereageerd. Zorgaanbieders zijn in de eerste plaats zelf verantwoordelijk voor het voldoen aan de normen voor informatiebeveiliging in de zorg, zoals de NEN7510. In deze wettelijke norm is benoemd dat het verplicht is een risicobeoordeling uit te voeren.[11] Onderdeel van deze risicobeoordeling is het in kaart brengen van risico's in de toeleveringsketen. Om zorgaanbieders te ondersteunen bij het voldoen aan de NEN normen biedt VWS op verschillende manieren ondersteuning. Zo zijn aan het Nederlands Normalisatie Instituut (NEN) middelen verstrekt voor het verzorgen van opleidingen, het ontwikkelen van implementatiehandvatten en het oprichten van een community waarin zorgmedewerkers van elkaar kunnen leren. De hulpmiddelen zijn kosteloos ter beschikking gesteld en ontwikkeld voor zowel organisaties die voor het eerst NEN 7510 implementeren als voor organisaties die NEN 7510 al geïmplementeerd hebben en moeten overstappen op de nieuwe versie van de norm. Daarnaast biedt Z-CERT, het expertisecentrum cybersecurity in de zorg, ondersteuningen door middel van het informeren over kwetsbaarheden in de software die wordt gebruikt door zorgaanbieders.
Het ATR adviseert om aan de hand van scenario's inzichtelijk en concreet te maken welke organisatie(s) in welke situatie verantwoordelijk zijn voor het doen van een melding. Hierop volgt de volgende toelichting. Het is belangrijk dat het duidelijk is voor entiteiten hoe zij dienen te voldoen aan de meldplicht. In de Cbw en het Cbb is er geen delegatiegrondslag opgenomen om nadere regels te stellen over de uitvoering van de meldplicht, anders dan welke informatie de entiteit dient te verstrekken bij het doen van melding. Er zal in interdepartementaal verband worden onderzocht hoe hier via een andere weg invulling kan worden gegeven aan dit advies.
Het ATR adviseert na één jaar een invoeringstoets te doen zodat tijdig kan worden bepaald of de invulling van de zorgplicht en criteria voor significante incidenten en de meldplicht passend en werkbaar zijn voor de zorgsector of bijsturing behoeft. Het volgende wordt hierop toegelicht. Kort na de inwerkingtreding van de regeling kan nog geen diepgaand beeld worden gekregen van de effecten

[11] NEN 7510:2024, Informatiebeveiliging in de zorg, artikel 6.1.2.

van de drempelwaarden, omdat er nog te weinig ervaring mee zal zijn opgedaan en dus ook geen gegevens kunnen worden geleverd. In het Cbb is in artikel 24, derde lid opgenomen dat ten minste elke vier jaar de doeltreffendheid van de drempelwaarden zal worden geëvalueerd. Voor de regeling zal er voor een evaluatietermijn van twee jaar worden gekozen. Voor de overige bepalingen zal worden aangesloten bij de evaluatietermijn van vijf jaar zoals deze is opgenomen in artikel 94 van de Cbw.
Het ATR adviseert toe te lichten of indirecte kosten (zgn. 'trickle down effecten') ook in de regeldruk-analyse zijn meegenomen. Als dit niet het geval is, dienen deze kosten alsnog in beeld te worden gebracht. De 'trickle down effecten' zijn niet meegenomen in de berekening omdat er volgens de huidige regelgeving geen specifieke verplichtingen zijn voor bedrijven onder de Cbw om aanvullende informatie van toeleveranciers te eisen. Essentiële en belangrijke entiteiten moeten op grond van de Cbw een beleid hebben voor de beveiliging van de toeleveringsketen. Dit beleid moet de afhankelijkheden identificeren van producten, diensten en leveranciers, die de veiligheid van hun netwerken kunnen beïnvloeden. Het beleid volgt een risk-based approach; de entiteiten beoordelen zelf welke leveranciers cruciaal zijn en welke eisen zij aan hen stellen. Het ontbreken van wettelijke verplichtingen leidt ertoe dat indirecte effecten niet vanuit wetgeving worden aangemerkt, maar eerder als een interne beslissing van de entiteiten.
Het ATR adviseert toe te lichten of in de regeldrukberekeningen ook het eventueel aannemen van nieuw personeel is meegenomen. In de regeldruktoets is naar voren gekomen dat organisaties verwachten te kunnen volstaan met eenmalige aanpassingen in de werkwijze en dat voor deze werkzaamheden het huidig personeel wordt aangevuld met externe inhuur. De geschatte inzet varieert van één voltijdmedewerker tot meerdere deeltijdmedewerkers. Daarnaast blijkt uit de regeldruktoets dat organisaties geen extern personeel verwachten aan te treken of externe kosten te maken met betrekking tot de meldplicht. In deze berekeningen zijn voornamelijk tijdsbestedingskosten meegenomen en geen expliciete verwachtingen op het aannemen van meer personeel met betrekking tot het uitwerken van de zorgplicht.

8.3 Toezichts- en handhavingstoets Inspectie Gezondheidszorg en Jeugd

De IGJ concludeert op basis van de uitgevoerde Toezicht- en Handhaafbaarheidstoets (hierna: T&H-toets) dat de voorgestelde regeling, bezien vanuit het perspectief van toezicht en uitvoering in de praktijk, geen aanpassing behoeft. Wel heeft de IGJ geadviseerd om de toelichting op twee onderdelen te verduidelijken.
Het eerste advies betreft de zinsnede in paragraaf 4.1 met betrekking tot de verplichting om te voldoen aan de NEN 7510. De toelichting zal op dit punt worden aangepast, waarbij de gevraagde verduidelijking wordt verwerkt.
Het tweede advies heeft betrekking op de vermelding in paragraaf 2.3, dat de regeling niet van toepassing zou zijn op entiteiten die onderzoek verrichten, zoals gedefinieerd in artikel 1, onderdeel f, van de WMO. De IGJ constateert dat deze definitie een onnodige beperking vormt voor de reikwijdte van de regeling. Zij merkt op dat ook verrichters van medisch-wetenschappelijk onderzoek onder de sector vallen van 'entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren naar geneesmiddelen' (bijlage 1 van de Cbw). De definitie in de toelichting zal op dit punt worden aangepast, waarbij het gestelde advies wordt overgenomen.

9. Inwerkingtreding

Deze regeling treedt in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin zij wordt geplaatst.

II. Artikelsgewijze toelichting

Hoofdstuk 1. Algemene bepalingen

Artikel 1.1 – Begripsbepaling

Op grond van artikel 1 van de Cbw en artikel 1 van het Cbb zijn de in die artikelen genoemde begrippen ook van toepassing op deze regeling. Met artikel 1.1 wordt daar een aantal begrippen aan toegevoegd.

Artikel 1.2 – Reikwijdte

Deze regeling is van toepassing op de in bijlage 1 van de Cbw beschreven sector gezondheidszorg en de in bijlage 2 van de Cbw omschreven subsector vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek. Deze subsector maakt onderdeel uit van de Sector Vervaardiging. Deze regeling is voor wat betreft laatstgenoemde sector enkel van toepassing op de

genoemde subsector. Dit is toegelicht in paragraaf 2.3.

Hoofdstuk 2. Nadere regels cyberbeveiliging

Artikel 2.1 – Maatregelen

In artikel 2.1, onderdeel a, wordt bepaald dat entiteiten in ieder geval de maatregelen als bedoeld in artikel 21, eerste lid, van de wet en hoofdstuk 4 van het besluit hebben genomen zodat deze maatregelen *aantoonbaarovereenkomen* met het bepaalde in de NEN 7510. Zoals toegelicht in paragraaf 4.1 van het algemeen deel van deze toelichting, moeten zorginformatiesystemen en elektronische uitwisselingsystemen van zorgaanbieders op grond van artikel 3 van het Besluit elektronische gegevensverwerking door zorgaanbieders reeds voor voldoen aan de NEN 7510. Deze NEN-norm kan door eenieder kosteloos worden ingezien. Hoewel de NEN 7510 gericht is op zorgaanbieders, kunnen ook andere entiteiten ervoor kiezen om te voldoen aan de NEN 7510.

Daarnaast is in artikel 2.1, onderdeel b, bepaald, dat entiteiten ook de maatregelen als bedoeld in artikel 21, eerste lid, van de wet en hoofdstuk 4 van het besluit kunnen laten overeenkomen met het bepaalde in de ISO 27001 en de ISO 27002.

In artikel 2.1, onderdeel c, is bepaald, dat indien de genomen maatregelen van entiteiten zoals bedoeld in artikel 21, eerste lid, van de wet en hoofdstuk 4 van het besluit niet voldoen aan de NEN 7510, of ISO 27001 en de ISO 27002, zij ook maatregelen kunnen nemen die een gelijkwaardig beschermingsniveau bieden. In dat geval moet de entiteit zelf aantonen dat er voldoende maatregelen zijn genomen, daarvan is in elk geval sprake als deze maatregelen een vergelijkbaar niveau van beveiliging bieden als de maatregelen die voortvloeien uit de ISO 27001 en de ISO 27002, of de NEN 7510.

Artikel 2.2 – Criteria significante incidenten

Artikel 2.2, eerste lid, bevat een uitwerking van de criteria voor significante incidenten in de zin van artikel 25, tweede lid, onderdeel a van de wet. Dit is omschreven in paragraaf 4.2.2.

Voor onderdeel d geldt dat er slechts sprake is van een significant incident indien de ernstige aantasting het gevolg is van een vermoedelijke kwaadwillende handeling. Hiermee wordt gedoeld op vermoedens van cybercriminaliteit, zoals hacks, diefstal of ransomaanval, phishing etcetera. Dat dit ook zo is, hoeft op het moment van melden nog niet vast te staan. Het vermoeden is reeds voldoende voor de meldplicht. Van een significant incident is tevens sprake indien een incident de gevolgen omschreven in het eerste lid kan veroorzaken of andere entiteiten heeft getroffen of kan treffen als bedoeld in art. 25, tweede lid, onderdeel b van de wet. Met dit lid wordt gedoeld op een incident dat tijdig wordt ontdekt en waar de schadelijke gevolgen worden voorkomen, maar dat hetwel had kunnen leiden in het eerste lid genoemde omstandigheden. Het derde lid verduidelijkt dat dit artikel niet van toepassing is indien sprake is van geplande gevolgen van geplande onderhoudswerkzaamheden die door of namens de essentiële entiteit of belangrijke entiteit worden uitgevoerd.

Artikel 2.3 tot en met 2.5 – Waarschuwing, melding en verslag

Zoals toegelicht in paragraaf 4.2.3 worden er in artikel 2.3 tot en met 2.5 nadere regels gesteld over de gegevens die aangeleverd moeten worden bij de vroegtijdige waarschuwing, de melding en het voortgangs- en eindverslag. Bij de melding en het voortgangs- en eindverslag gaat het onder meer om informatie over gevolgen van het incident voor en betrokkenheid bij het incident van leveranciers aan de entiteit en afnemers van producten en diensten van de entiteit.

Hoofdstuk 3 aanwijzing autoriteit en toezichthouder

Artikel 3.1- Aanwijzing autoriteit

Op grond van het nieuwe artikel 3.1 worden de ambtenaren van de IGJ die zijn belast met het toezicht op de naleving van deze wet, aangewezen als autoriteit. Deze expliciete aanwijzing is ter verduidelijking voor de praktijk. De autoriteit werkt samen met de andere autoriteiten, CSIRTS en het centrale contactpunt om, ook kunnen zij op grond artikel 51 e.v. van de Cbw onderling noodzakelijke gegevens uitwisselen.

Artikel 3.2 – Aanwijzing toezichthouder

Op grond van artikel 68 van de Cbw wijst de bevoegde autoriteit een ambtenaren aan die belast is met het toezicht op het bepaalde bij of krachtens de Cbw en het bepaalde op grond van in de richtlijn aanwezen uitvoerings- en gedelegeerde handelingen. In dit artikel worden de ambtenaren van de IGJ

aangewezen als deze ambtenaren. Zij zijn daarom belast met het toezicht op de naleving van de hiervoor genoemde bepalingen.

Hoofdstuk 4. Slotbepalingen

Artikel 4.1 Inwerkingtreding

Deze regeling treedt in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin zij wordt geplaatst.

Artikel 4.2 Citeertitel

Er zijn diverse ministeriële regelingen die vallen onder de Cbw, daarom is gekozen om de onderhavige regeling de citeertitel ‘Cyberbeveiligingsregeling voor de zorg’ te geven.

De Minister van Langdurige zorg, Jeugd en Sport,
W.R.C. Sterk