Toelichting

I. Algemeen deel van de nota van 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. Daarnaast wordt de stichting Z-CERT (hierna: Z-CERT) aangewezen als sectoraal Computer Incident Response Team (hierna: CSIRT) voor de sector gezondheidszorg en de subsector vervaardiging onder de Cbw en worden hier regels over gesteld.

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 middels 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 voor de meest kwetsbaren 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 en subsector. 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 alleen jeugdhulp of maatschappelijke ondersteuning aanbieden, niet onder de Cbw, Cbb en deze regeling vallen. Entiteiten die jeugdhulp of maatschappelijke ondersteuning aanbieden

en daarnaast ook zorg verlenen die onder de Wkkgz valt, worden wel aangemerkt als zorgaanbieder.

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 lid 1, onder 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 lid 1 onder o van de Wet medisch onderzoek met mensen (hierna: WMO). Deze regeling geldt niet voor entiteiten die onderzoek verricht zoals gedefinieerd in artikel 1, onder f, van de WMO.

Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen vervaardigen
Het betreft in ieder geval entiteiten die onder de Geneesmiddelenwet als de fabrikanten worden aangemerkt. De farmaceutische basisproducten zijn de grondstoffen die worden gebruikt bij de productie van geneesmiddelen voor humaan gebruik. Voor wat betreft farmaceutische bereiding heeft dit betrekking op grootschalige magistrale bereidingen en de vervaardiging van geregistreerde geneesmiddelen.

Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek
Het betreft hier entiteiten die medische hulpmiddelen of in-vitrodiagnostiek vervaardigen zoals bedoeld in artikel 2, onderdeel 1 van de Verordening 2017/745 en artikel 2, onderdeel 2 van de Verordening 2017/746. Deze entiteiten zijn ongeacht de grootte en omvang geclassificeerd als belangrijke entiteiten zoals op genomen in bijlage 2, met uitzondering wanneer zij medische hulpmiddelen vervaardigen in het kader van een noodsituatie waarvoor de Europees geneesmiddelenbureau (hierna: EMA) een lijst opstelt op het moment dat zich een ramp of crisis voordoet. Het gaat hierbij dus niet om entiteiten die uitsluitend hulpmiddelen importeren of distribueren.

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
Hieronder vallen entiteiten die in een noodsituatie medische hulpmiddelen vervaardigen. Het EMA is belast met het opstellen van een lijst met kritieke medische hulpmiddelen in noodsituaties op het gebied van de volksgezondheid. De EMA is onder meer de Europese autoriteit voor paraatheid op gezondheidsnoodsituaties maar heeft op dit moment deze lijst nog niet vastgesteld. Dit betekent dan ook dat er op het moment dat er geen noodsituatie is afgekondigd door de EMA, er ook géén partijen als essentiële entiteit onder deze categorie worden aangemerkt. Gezien vervaardigers van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek als belangrijke entiteiten in bijlage 2 onder de Cbw vallen, betekent het in de praktijk dat entiteiten die kritieke hulpmiddelen vervaardigen in noodsituaties daardoor als essentiële entiteiten zullen worden aangemerkt zodra de lijst is vastgesteld.

3. Het CSIRT

3.1 Aanwijzing Z-CERT als Sectoraal CSIRT
Op grond van artikel 2, tweede lid, Cbb wordt Z-CERT aangewezen als sectorale CSIRT voor de sector gezondheidszorg en de subsector vervaardiging. Z-CERT is in 2017 opgericht op initiatief van de Nederlandse Vereniging van Ziekenhuizen (hierna: NVZ), Nederlandse Federatie van Universitair Medische Centra (hierna: NFU) en GGZ Nederland (hierna: GGZ). Z-CERT heeft geen winstoogmerk en is het expertisecentrum op het gebied van cybersecurity in de zorg.

Z-CERT fungeert al sinds 2017 als Computer Emergency Response Team (hierna: CERT) voor de zorg en heeft sinds de inwerkingtreding van de NIS2-richtlijn op 17 oktober 2024 al enkele taken van CSIRT voor de zorg op zich genomen. Dit betekent dat veel processen, systemen en kennis al zijn opgebouwd om haar wettelijke taken uit te voeren voor het zorgveld. Momenteel werkt Z-CERT met individuele deelnemersvergoedingen en mantelovereenkomsten met koepelorganisaties binnen de zorg. Dit betekent dat instellingen ofwel zelfstandig ofwel via hun koepel een vergoeding betalen voor de dienstverlening van Z-CERT. Zodra de Cbw in werking is getreden krijgt Z-CERT wettelijke taken en zal dit dus veranderen. Alle organisaties die binnen de sector zorg onder de Cbw vallen, hebben recht op de in de Cbw beschreven ondersteuning door Z-CERT. Het ministerie van Volksgezondheid, Welzijn en Sport (hierna: VWS) zal Z-CERT hiervoor bekostigen.

3.2 Governance
De aanwijzing van Z-CERT als CSIRT betekent dat deze organisatie te maken krijgt met de uitvoering van wettelijk taken. Het uitgangspunt hierbij is dat Z-CERT vanwege haar specifieke deskundigheid is aangewezen en met haar bestaande kennis van cybersecurity in de zorg invulling kan geven aan haar wettelijke taken. Onverlet de eigen verantwoordelijkheid van Z-CERT is het echter nodig dat er randvoorwaarden gelden voor de uitoefening van deze taken. Deze randvoorwaarden zien op de goede uitvoering van de wettelijke taken en de continuïteit daarvan. Ze zijn onderwerp van gesprek tussen de minister van VWS en Z-CERT. De eisen worden in deze regeling opgenomen.
De randvoorwaarden zien deels op de inrichting van de organisatie en deels op de verantwoording van de financiële middelen en de taakuitoefening. De beleidsprioriteiten en doelstellingen zullen in ieder geval worden vastgelegd in een jaarplan. Dit biedt transparantie voor zowel de minister van VWS als de organisaties in het zorgveld. Ook wordt in de regeling vastgelegd dat de Minister van VWS, indien gewenst, alle benodigde informatie bij en over Z-CERT kan opvragen. Dit kan bijvoorbeeld gaan om financiële of beleidsmatige gegevens die verband houden met de uitvoering van de wettelijke taak, of om informatie over incidenten in de zorgsector. Ook indien Z-CERT een besluit neemt binnen de organisatie die de uitoefening van haar wettelijke taken raakt (bijvoorbeeld het veranderen van rechtsvorm), dient zij voorafgaand aan het besluit de minister schriftelijk te consulteren. Daarnaast wordt voorzien in een regeling bij ernstige taakverwaarlozing. De te geven aanwijzingen hebben als doel dat de uitvoering van wettelijke taken gegarandeerd blijft.

Ingevolge deze regeling zal Z-CERT meer organisaties met verschillende soorten dienstverlening ondersteunen. Organisaties die onder de Cbw vallen zijn verplicht zich te registreren in het NCSC-portaal op het moment dat de Cbw in werking treedt. De bestaande systemen van Z-CERT zullen op dit portaal worden aangesloten. Eén van de eerste prioriteiten van Z-CERT is om deze toename in organisaties te verwerken.

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 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 een gelijkwaardig beschermingsniveau bieden met het bepaalde in de NEN 7510, en de ISO 27001 en de ISO 27002.

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 van verwachting dat zij deze norm zullen hanteren bij het voldoen aan de verplichtingen die voortvloeien uit de Cbw.
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 zorgaanbieders, 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

Een incident wordt als significant beschouwd wanneer het aan één van de in artikel 3.2 van deze regeling genoemde drempelwaarden 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 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) niet-beschikbaarheid van diensten, worden niet als significante incidenten beschouwd.

4.2.2 Drempelwaarden 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 kan dit verreikende 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. Volgens de Cbw is er sprake van een incident significant als het (i) een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of (ii) als het andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. In deze regeling worden er zorgspecifieke drempelwaarden opgesteld om hier verdere invulling aan te geven.

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 kritieke bedrijfsmiddelen, kritische bedrijfsprocessen en bedrijfsgevoelige informatie. Dit sluit aan bij de verplichting zoals opgenomen in artikel 15 van het Cbb, voor een entiteit om haar 'assets' te classificeren en hiervan een inventaris te creëren. Het vaststellen van kritische bedrijfsprocessen vormt een belangrijk onderdeel van de risicobeoordeling. 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 overschreven, wordt het incident beschouwd als significant en dient een entiteit altijd melding te doen van het incident.

a. Een kritisch bedrijfsproces ligt langer dan 4 uur gedeeltelijk of geheel stil

Een incident dat leidt tot een gedeeltelijke of volledige verstoring van het kritisch bedrijfsproces die langer dan 4 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. Een gedeeltelijke of volledige verstoring van een kritisch bedrijfsproces langer dan 4 uur wordt gezien als een ernstige operationele verstoring van de dienstverlening en kan mogelijk ernstige gevolgen hebben voor patiënten. Bij een gedeeltelijke of volledige verstoring van het proces moet in ieder geval 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 4 uur. Een gedeeltelijke verstoring kan ook betekenen dat er langer dan 4 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.

Als voorbeeld kan men 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 verstoord 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 ernstig 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 ernstige 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 ernstige 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 ernstig aangetast ten gevolge van een vermoedelijke kwaadwillende handeling

Als een incident als gevolg heeft dat de vertrouwelijkheid van bijzondere persoonsgegevens ernstig 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 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.

Een belangrijke vorm van bijzondere persoonsgegevens binnen de zorg zijn patiënt- en cliëntgegevens. In de zorg wordt er gewerkt met uiterst gevoelige informatie over personen. Deze informatie wordt in steeds grotere mate digitaal opgeslagen en elektronisch uitgewisseld tussen partijen. Het openbaar worden van dergelijke informatie over patiënten kan een ernstige inbraak zijn op de persoonlijke levenssfeer van een patiënt of cliënt. Daarnaast kan de schending van vertrouwelijke medische informatie over patiënten grote maatschappelijke onrust met zich meebrengen en het vertrouwen in de zorg schaden.

Datalekken waarbij persoonsgegevens betrokken zijn dienen mogelijk eveneens gemeld te worden bij de Autoriteit Persoonsgegevens op grond van de Algemene Verordening Gegevensbescherming (hierna: AVG). In het kader van de Cbw gaat het alleen om digitale gegevens – toegankelijk via netwerk- en informatiesystemen – waarbij de vertrouwelijkheid ernstig is aangetast ten gevolg is van een vermoedelijke kwaadwillende handeling. Om te bepalen of iets een ernstige aantasting is moet worden rekening gehouden met het aantal personen dat is geraakt en de gevoeligheid van de informatie.

Dit betekent dat een cyberincident waarbij er een inbreuk is gemaakt op persoonsgegevens in sommige, maar niet alle gevallen, zowel kan worden gezien als een datalek 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 of overlijden van een persoon, dan dient dit gemeld te worden. Het kan hierbij bijvoorbeeld gaan om een cyberaanval waarbij het proces kortstondig (korter dan 4 uur) wordt verstoord, maar waarbij er wel redelijkerwijs te vermoeden is dat er als gevolge 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 het incident nog niet heeft plaatsgevonden, bestaat er wel een reëel risico. Het onaanvaardbare risico op blijvend letsel, ziekenhuisopname of overlijden is enkel meldingswaardig als dit een gevolg is van een cyberincident of verstoring van de netwerk en informatiesystemen.

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 Z-CERT als de IGJ in de verschillende fases van het incident. Dit helpt de IGJ en Z-CERT 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.

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 Z-CERT 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 Z-CERT 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 overlegd.

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 Z-CERT is er rekening gehouden met de bestaande praktijken bij de IGJ en Z-CERT 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.[1] 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.[2] 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.

[1] Het rapport is nog niet definitief vastgesteld. Het is mogelijk dat er nog kleine wijzigingen in de berekeningen worden doorgevoerd.

[2] 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.

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 getracht een MKB-toets uit te voeren. Echter er was geen animo en waren 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.[3]

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[4], de Wkkgz[5] en het Begz[6] reeds verplicht zijn om te voldoen aan de beveiligingsvoorschriften zoals vastgelegd in de NEN7510.[7] 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.[8] 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 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.

[3] KCBR, Handboek Meting Regeldrukkosten, 29 november 2023

[4] Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg

[5] Wet kwaliteit, klachten en geschillen zorg

[6] Besluit elektronische gegevensverwerking door zorgaanbieders

[7] 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).

[8] https://z-cert.nl/actueel/nieuws/cbweetje-de-nen7510-en-de-zorgplicht

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 1. 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 2. 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**

<u>Meldplicht</u>

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 Z-CERT 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 3. 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 4. 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 een sectoraal CSIRT voor de zorg aan te wijzen. Deze rol wordt in deze regeling bij stichting Z-CERT belegd. 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 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

8.1 Internetconsultatie
PM Consultatie en toetsing

8.2 Advies Adviescollege toetsing regeldruk (tenzij al vermeld bij de beschrijving van de regeldruk)
PM Consultatie en toetsing

8.3 Toezichts- en handhavingstoets Inspectie Gezondheidszorg en Jeugd
PM Consultatie en toetsing wordt pas opgenomen na de internetconsultatie

9. Inwerkingtreding

Deze regeling moet in samenhang worden gezien met de Cbw, het Cbb en de ministeriële regeling PM (van Justitie). Deze regeling treedt daarom op hetzelfde moment inwerking als de Cbw en het Cbb. Naar verwachting is dit PM.

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 worden 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. CSIRT

Artikel 2.1 Aanwijzing CSIRT
Op grond van artikel 2, eerste lid, van het Cbb kan bij ministeriële regeling voor een specifieke sector of subsector een CSIRT aangewezen worden. Op grond van artikel 3.1 van deze regeling wordt Stichting Z-CERT aangewezen als het CSIRT voor de sector gezondheidszorg en de subsector vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek. In paragraaf 3.1 van het algemeen deel van de toelichting is uitgelegd waarom voor deze stichting is gekozen.

Artikel 2.2 Governance
Om de goede uitvoering van de wettelijke taken van het CSIRT te borgen worden er aantal regels gesteld aan de governance van de stichting. Zo moet in de statuten worden geborgd dat er een onafhankelijke en deskundige raad van toezicht is en dat de raad van toezicht de bevoegdheid heeft om het bestuur in te stellen en bestuursleden te ontslaan. Het CSIRT kan enkel haar statuten wijzigen met instemming van de minister.

Artikel 2.3 Verantwoording
In artikel 2.3 wordt de verantwoording over de werkzaamheden vastgelegd. Het CSIRT stuurt jaarlijks een begroting en een jaarplan op en een kopie van de vastgestelde jaarrekening en het bestuursverslag. Deze documenten dienen als input voor de gesprekken tussen de minister en het CSIRT. Die gesprekken zullen in de regel plaatsvinden met het bestuur, maar indien de minister dat noodzakelijk acht, kan ook met de raad van toezicht worden gesproken. Om de juistheid van de gegevens te waarborgen, wordt bepaald dat de jaarrekening en het bestuursverslag worden gecontroleerd door een registeraccountant of een accountant administratieconsulent in de zin van artikel 2:393 van het Burgerlijk Wetboek.
Voorts is van belang dat er voldoende transparantie bestaat over eventuele nevenwerkzaamheden van het CSIRT. Daarom is opgenomen dat het CSIRT jaarlijks aan de minister inzage in de aard en omvang van deze werkzaamheden verschaft. Verder is van belang dat het CSIRT de minister of de door de minister aangewezen toezichthouders alle inlichtingen verschaft die van belang zijn voor de uitvoering van de wettelijke taken van de minister.
In het geval dat het CSIRT voornemens is besluiten te nemen die van wezenlijke invloed zijn op de uitoefening van de taken als CSIRT. Gedacht kan bijvoorbeeld worden aan het starten van bepaalde nevenwerkzaamheden of wijziging in het bestuur of de raad van toezicht of het veranderen van de rechtsvorm.

Artikel 2.4 Taakverwaarlozing
Om te borgen dat de wettelijke taken te allen tijde goed worden uitgeoefend, kan onze minister de stichting algemene en specifieke aanwijzingen geven in het geval de stichting de uitvoering van haar wettelijke taken verwaarloost. Deze aanwijzingen zijn er op gericht dat de wettelijke taken zo spoedig mogelijk weer effectief worden uitgevoerd.

Artikel 2.5 Andere activiteiten
Het CSIRT kan naast haar wettelijke taken ook andere activiteiten ontplooien. Het is evenwel van belang dat deze activiteiten niet kunnen interfereren met de uitoefening van de wettelijke taken. In artikel 3.5 wordt daarom bepaald dat het CSIRT indien deze activiteiten de uitvoering van de wettelijke taken kunnen belemmeren of beïnvloedden.

Artikel 2.6 Continuïteit
In het geval de rechtspersoon die het CSIRT in stand houdt zich wil opheffen, dient de minister hiermee in te stemmen. Zo wordt geborgd dat de minister de wettelijke taken eerst elders kan onderbrengen, alvorens het CSIRT zich opheft. In het geval het CSIRT wordt opgeheven of als een andere entiteit wordt aangewezen als CSIRT, draagt het CSIRT de archiefbescheiden en systemen over aan de minister. Het gaat hier om de systemen die noodzakelijk zijn voor de uitvoering van de wettelijke taken.

Hoofdstuk 3. Nadere regels cyberbeveiliging

Artikel 3.1 – Maatregelen
In artikel 3.1, onderdeel a, wordt bepaald dat entiteiten in ieder geval de maatregelen als bedoeld in artikel 21, eerste lid, van de wet hebben genomen zodat deze maatregelen *overeenkomen* 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 3.1, onderdeel b, bepaald, dat entiteiten ook de maatregelen als bedoeld in artikel 21, eerste lid, van de wet kunnen laten overeenkomen met het bepaalde in de ISO 27001 en de ISO 27002.

In artikel 3.1, onderdeel c, is bepaald, dat indien de genomen maatregelen van entiteiten zoals bedoeld in artikel 21, eerste lid, van de wet 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 3.2 – Criteria significante incidenten
Artikel 3.2 bevat criteria voor significante incidenten. 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. Hiermee wordt gedoeld op een incident dat tijdig wordt ontdekt en waar de schadelijke gevolgen worden voorkomen, maar dat wel 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 3.3 tot en met 3.5 – waarschuwing, melding en verslag
Zoals toegelicht in paragraaf 4.2.3 worden er in artikel 3.3 tot en met 3.5 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 4 aanwijzing autoriteit en toezichthouder

Artikel 4.1
Op grond van het nieuwe artikel 4.1 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 4.2
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 5. Slotbepalingen

Artikel 5.1 Inwerkingtreding
Voor de inwerkingtreding van deze regeling is aansluiting gezocht bij de inwerkingtreding van de Cbw. Dat betekent dat deze regeling in werking treedt als artikel 1 van de Cbw in werking treedt.

Artikel 5.2 Citeertitel
Er zijn diverse regelingen die vallen onder de Cbw, daarom is gekozen om de onderhavige regeling de citeertitel 'Cyberbeveiligingsregeling zorg' te geven.

De Minister van Volksgezondheid,
Welzijn en Sport,