Adviescollege toetsing regeldruk

Aan de minister van Volksgezondheid, Welzijn en Sport
De heer prof. dr. J.A. Bruijn
Postbus 20350
2500 EJ DEN HAAG

Onze referentie
MvH/RvZ/ATR4264/2025-U200

Uw referentie

Datum
18 december 2025

Onderwerp
Cyberbeveiligingsregeling Zorg

Geachte heer Bruijn,

Op 10 november 2025 is de *Cyberbeveiligingsregeling zorg* voor advies voorgelegd aan het Adviescollege toetsing regeldruk (ATR). De adviestermijn loopt tot en met 22 december.

Context

Nederland dient de Europese richtlijnen *Network and Information Security Directive* (NIS2-richtlijn) en de *Critical Entities Resilience Directive* (CER-richtlijn) in Nederlandse wet- en regelgeving te implementeren. De NIS2 richtlijn introduceert maatregelen om de digitale veiligheid van belangrijke systemen te vergroten, terwijl de CER-richtlijn maatregelen betreft om de weerbaarheid te vergroten ten aanzien van andere risico's, zoals fysieke sabotage en natuurrampen. Voor de nationale implementatie van de NIS2-richtlijn zijn eerder de Cyberbeveiligingswet (Cbw) en het Cyberbeveiligingsbesluit (Cbb) door ATR van advies voorzien (in combinatie met de Wet weerbaarheid kritieke entiteiten (Wwke) en Besluit weerbaarheid kritieke entiteiten (Bkke) ten behoeve van implementatie van de CER-richtlijn).[1]

De NIS2-richtlijn, de Cbw en Cbb werken diverse verplichtingen uit voor zogenaamde essentiële en belangrijke entiteiten tot het nemen van maatregelen om de risico’s voor hun netwerk- en informatiesystemen te beheersen. De regelgeving heeft betrekking op entiteiten die op basis van een aantal (in de richtlijn bepaalde) criteria over dienstverlening, schaalgrootte of organisatietype worden onderscheiden. Te nemen maatregelen richten zich op digitale (cyber)risico’s voor netwerk- en informatiesystemen, zoals het internet en het betalingsverkeer. De verplichtingen omvatten onder meer een zorgplicht en een meldplicht.

[1] Zie https://www.adviescollegeregeldruk.nl/documenten/2024/07/01/atr-advies-wetsvoorstellen-cyberbeveiligingswet-cbw-en-de-wet-weerbaarheid-kritieke-entiteiten-wwke en https://www.adviescollegeregeldruk.nl/documenten/2025/04/04/atr-advies-cyberbeveiligingsbesluit-en-besluit-weerbaarheid-kritieke-entiteiten.

Contact:
Postbus 16228
2500 BE DEN HAAG
Bezoekadres: Rijnstraat 50
2515 XP DEN HAAG
info@atr-regeldruk.nl
www.adviescollegeregeldruk.nl
Tel: 070-310 86 66

De reikwijdte van de bovenliggende wetten en besluiten is sectoroverstijgend. 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 in een ministeriële regeling nadere sectorale uitwerking te geven aan de zorgplicht en meldplicht. De voorliggende ministeriële regeling bevat deze sectorspecifieke bepalingen voor de zorg. De verschillende sectorale regelingen zijn waar relevant door het college in samenhang bezien. Daarbij acht het college het van belang om te benadrukken dat het gehele wetgevingspakket inzake Cyberbeveiliging een grote inspanning van diverse sectoren vraagt met forse regeldrukgevolgen (ruim één miljard euro). Sectoren moeten bovendien al op korte termijn gaan voldoen aan de regelgeving: de inwerkingtreding is in 2026 voorzien. Nut en noodzaak van cyberbeveiliging staan niet ter discussie. De sectorale regelingen en de toelichtingen dienen echter de abstracte, juridische kaders zodanig te concretiseren dat deze kenbaar, werkbaar en haalbaar zijn voor de betreffende sectoren. Het college constateert in de diverse adviezen dat de verschillende sectorale regelingen deze mate van concretisering nog niet bevatten. Het risico bestaat hiermee dat beleidsdoelen niet worden verwezenlijkt.

Inhoud van het voorstel

De regeling werkt voor de sector gezondheidszorg en de subsector vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor invitrodiagnostiek (subsector vervaardiging) de volgende onderdelen uit:
1. Zorgplicht: Voor essentiële en belangrijke entiteiten als bedoeld en afgebakend in 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 te beheersen. Deze verplichting wordt de zorgplicht genoemd. De regeling bepaalt dat zorgorganisaties voor de uitvoering van de maatregelen zoals bedoeld de Cbw moet voldoen aan hetgeen is bepaald in de bestaande normen NEN 7510, of de ISO 27001 en de ISO 27002.
2. Meldplicht en drempelwaarden voor significante incidenten: De Cbw bevat een grondslag voor de uitwerking van een meldplicht bij significante incidenten. De regeling bevat een aantal drempelwaarden die bepalen wanneer sprake is van een significant incident.
3. Stichting Z-CERT (Z-CERT) wordt aangewezen als sectoraal Computer Incident Response Team (CSIRT) voor de sector gezondheidszorg en de subsector vervaardiging onder de Cbw. De regeling bevat bepalingen over de governance van deze stichting.
4. De IGJ wordt aangewezen als toezichthouder.

Het advies ziet hoofdzakelijk op de onderdelen genoemd onder 1 en 2, omdat hier regeldruk uit voortkomt.

Toetsingskader

ATR beoordeelt de regeldrukgevolgen aan de hand van het volgende toetsingskader:
1. Nuloptie (nut en noodzaak): is er een taak voor de overheid en is wetgeving het meest aangewezen instrument?
2. Zijn er minder belastende alternatieven mogelijk?
3. Is gekozen voor een uitvoeringswijze die werkbaar is voor de doelgroepen die de wetgeving moeten naleven?
4. Zijn de gevolgen voor de regeldruk volledig en juist in beeld gebracht?

1. Nut en noodzaak

De regeling geeft een nadere concretisering van de eisen en verplichtingen die voortvloeien uit de NIS2-richtlijn en de implementatieregelgeving Cbw en Cbb. Nut en noodzaak van de diverse verplichtingen zijn bij de richtlijn zelf en de eerdere ATR-adviezen over wet en besluit al aan de orde gekomen. De NIS2-richtlijn en de bijbehorende implementatie hebben als doel de verbetering van de digitale weerbaarheid van o.a. de sector gezondheidszorg en subsector vervaardiging. In deze sector en subsector heeft uitval of verstoring van de dienstverlening direct invloed op de continuïteit van zorg voor de meest kwetsbaren in de 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.

Het college ziet geen aanleiding voor opmerkingen onder nut en noodzaak.

2. Minder belastende alternatieven

Zorgplicht

Het college constateert dat in de regeling is gekozen om de zorgplicht nader in te vullen door aan te sluiten bij bestaande normen. Een entiteit moet voor de uitvoering van zorgplicht voldoen de NEN 7510, of de ISO 27001 en de ISO 27002. Deze normen zijn bekend en openbaar toegankelijk. 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. Hiermee wordt volgens de toelichting nadrukkelijk de keuze gemaakt om aan te sluiten op bestaande wettelijke normen. Zo wordt volgens het voorstel extra regeldruk voorkomen en worden organisaties binnen de zorg geholpen om op een eenduidige manier hun informatiebeveiliging en digitale weerbaarheid te verbeteren. Het college acht deze concrete invulling van de zorgplicht in algemene zin positief voor de werkbaarheid en de beperking van de regeldruk. Desondanks ziet het aanleiding voor enkele aandachtspunten over minder belastende alternatieven.

Het eerste aandachtspunt ziet op de samenhang met andere sectorale cyberbeveiligingsregelingen. Deze zijn gelijktijdig met de voorliggende regeling voor de zorg in (internet)consultatie gebracht. Voor sommige entiteiten geldt dat zij in meerdere sectoren actief zijn. In dat geval moeten zij de regels uit meerdere ministeriële regelingen in acht te nemen om aan de zorgplicht te voldoen. Daarbij kunnen zij te maken krijgen met verschillende bevoegde autoriteiten of CSIRT's. De toelichting bevat geen nadere onderbouwing hoe dubbele (toezichts)lasten worden voorkomen. Ook bevat de toelichting geen duiding van de samenhang met deze andere regelingen en de daarin gekozen (verschillende) invulling van de zorgplicht.

2.1 Het college 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.

Een belangrijk onderdeel van de zorgplicht is de verplichting voor essentiële en belangrijke entiteiten om conform de Cbw hun toeleveringsketen beveiligen. Hiervoor moet beleid schriftelijk

worden vastgesteld en toegepast, waarin de omgang wordt bepaald met (afhankelijkheden van) producten en diensten van leveranciers en dienstverleners die de beveiliging van netwerk- en informatiesystemen kunnen beïnvloeden. Bovendien moet de entiteit 'regelmatig' toetsen of rechtstreekse leveranciers voldoen aan de eisen die de entiteiten opstellen met betrekking tot de beveiliging van hun netwerk- en informatiesystemen. Onduidelijk is wat 'regelmatig' inhoudt. Of maatregelen daarbij 'passend en evenredig' zijn, is iets wat een toezichthouder kan bepalen als een organisatie op de ketenbeveiligingszorgplicht gecontroleerd wordt. Ook hier dienen verschillen tussen toezichthouders en stapeling van toezicht zoveel mogelijk voorkomen te worden. Het is in de regeling onduidelijk hoe risicogericht en proportioneel toezicht wordt vormgegeven.

2.2 Het college adviseert nader toe te lichten hoe risicogericht en proportioneel toezicht vormgegeven wordt en op welke wijze stapeling van toezicht wordt voorkomen.

Meldplicht bij significante incidenten

Essentiële en belangrijke entiteiten moeten op grond van de Cbw alle significante incidenten melden. In het Cbw is bepaald dat een incident significant is als het een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken, of andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. De regeling bevat voor de zorgsector nadere criteria op basis waarvan wordt bepaald of sprake is van een significant incident (drempelwaarden). Dat is het geval als een kritisch bedrijfsproces voor langer dan 4 uur stilligt, als kritieke bedrijfsmiddelen beschadigd zijn, als de integriteit, vertrouwelijkheid of beschikbaarheid van bedrijfsgevoelige informatie of de vertrouwelijkheid van bijzondere persoonsgegevens zijn aangetast, of als er sprake zijn van blijvend letsel, ziekenhuisopname of overlijden. Ook bevat het verplichtingen voor 'bijna-incidenten': het kan hier gaan om incidenten waarbij er een onaanvaardbaar *risico* ontstaat op blijvend letsel, ziekenhuisopname of overlijden van een persoon. Indien één van de drempelwaarden wordt overschreden, wordt het incident beschouwd als significant en dient een entiteit altijd melding te doen van het incident. Het college merkt op dat de toelichting geen transparante afweging en onderbouwing bevat hoe de drempelwaarden tot stand zijn gekomen en of mogelijk minder belastende alternatieven zijn overwogen. Het college constateert dat sommige drempelwaarden (vooral) voor kleinere organisaties belastend kunnen zijn. Hoewel organisaties met minder dan 50 werknemers door de richtlijn uitgezonderd zijn van de verplichtingen, zijn organisaties met iets meer dan 50 werknemers wel degelijk te beschouwen als kleinere organisaties. Zo betekent de drempelwaarde om bij een incident van langer dan 4 uur binnen 24 uur te moeten melden dat kleinere organisaties mogelijk extra weekenddiensten moeten inroosteren en in sommige gevallen extra personeel moeten aannemen. Daar komt het knelpunt bij dat ICT-personeel schaars is. De vraag is daarmee in hoeverre deze eisen haalbaar zijn (zie ook toetsvraag 3). De regeling maakt niet duidelijk of er differentiatie (uitzonderingen) mogelijk is voor kleinere partijen of dat er minder belastende drempelwaarden mogelijk zijn. Te denken valt dat incidenten pas meldingsplichtig worden bij een langere duur dan de (nu niet onderbouwde) drempelwaarde van 4 uur.

2.3 Het college adviseert te onderbouwen hoe de drempelwaarden tot stand zijn gekomen en welke mogelijk minder belastende alternatieven zijn overwogen. Daarbij dient de toelichting specifiek in te gaan op de praktische uitvoerbaarheid van de drempelwaarden voor kleinere zorgorganisaties.

De toelichting bevat bij de meldplicht geen duiding van de samenhang met andere regelingen en de daar gehanteerde drempelwaarden. Als een entiteit in meerdere sectoren valt, moet de entiteit volgens de toelichting rekening houden met alle drempelwaarden die voor de verschillende sectoren gelden. Dit doet de vraag rijzen in hoeverre dit een (onnodige) stapeling van meldingen en toezichtslasten oplevert. Het risico op (onnodige) dubbele meldingen bestaat overigens ook als entiteiten niet onder meerdere sectoren vallen. Zo dienen incidenten omtrent data bij meerdere autoriteiten gemeld te worden. Organisaties hebben behoefte aan meer duidelijkheid ten aanzien van de vraag wanneer incidenten bij de IGJ/Z-CERT gemeld dienen te worden, wanneer bij de Autoriteit Persoonsgegevens, en wanneer bij allebei. Heldere voorschriften hierover kunnen onnodige (dubbele) meldingen beperken. Ook kan volgens het college één centraal portaal voor meldingen uitkomst bieden. Een dergelijk centraal meldpunt kan nationaal worden vormgegeven maar ook internationaal (Europees). Dit laatste is vooral van belang voor entiteiten die grensoverschrijdend werken en te krijgen met cyberincidenten die hun activiteiten in meerdere lidstaten raken. Deze organisaties hebben baat bij een Europees meldpunt. Dit meldpunt kan op zijn beurt informatie delen met nationale meldpunten zoals het IGJ en Z-CERT.

2.4 Het college 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.

De richtlijn bepaalt dat als sprake is van een incident, een essentiële entiteit binnen 24 uur een vroegtijdige waarschuwing moet doen aan haar Computer Security Incident Response Team (CSIRT) en de bevoegde autoriteit. Deze vroegtijdige melding moet vervolgens binnen 72 uur worden opgevolgd met een melding bij de CSIRT en de bevoegde autoriteit, met een update van de informatie in de vroegtijdige waarschuwing, een vroegtijdige beoordeling van het incident en de ernst en gevolgen hiervan, de indicatoren voor de aantasting en alle beschikbare informatie die het CSIRT en de bevoegde autoriteit kunnen gebruiken om eventuele grensoverschrijdende gevolgen van het incident te bepalen. Vervolgens moet de essentiële of belangrijke entiteit op verzoek van haar CSIRT of bevoegde entiteit een tussentijds verslag opstellen met nadere updates. Ten slotte moet de kritieke entiteit uiterlijk een maand na de eerdergenoemde melding een eindverslag indienen bij de CSIRT en de bevoegde autoriteit. Het college constateert dat de regeling nadere eisen bevat over 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 van afnemers van producten en diensten van de entiteit. Het college constateert dat hiermee sprake is van extra eisen ten opzichte van de richtlijn en hetgeen bij wet en besluit is bepaald. Onduidelijk is waarom deze extra eisen noodzakelijk zijn. Hiermee is er sprake van een nationale kop. Het college constateert bovendien dat de regeling ook extra eisen bevat ten opzichte van andere sectorspecifieke regelingen. Een motivering van ook dit verschil ontbreekt.

2.5 Het college adviseert nader te onderbouwen waarom de regeling een nationale kop zet op de rapportageverplichtingen voor zorgorganisaties. Indien er geen inhoudelijke redenen zijn voor deze nationale kop, dan adviseert het college de betreffende bepalingen te schrappen.

3. Werkbaarheid

Bij het advies bij de bovenliggende wet en besluit is door het college al aandacht gevraagd voor de praktisch uitwerking voor entiteiten. Het college adviseerde te waarborgen dat organisaties weten wat de verplichtingen precies inhouden en hoe die nageleefd moeten worden. De voorliggende regeling betreft de sectorale uitwerking van wet en besluit en is daarmee de geëigende plek om maatregelen te concretiseren en de werkbaarheid te borgen c.q. te onderbouwen. Onder toetsvraag 2 is al op diverse aspecten gevraagd om een concrete uitwerking en invulling van verplichtingen alsook om proportioneel toezicht om onnodige regeldruk te voorkomen. Deze adviespunten zien ook op het vergroten van de werkbaarheid voor zorgorganisaties, bijvoorbeeld als het gaat om duidelijkheid over de meldplicht. Het college acht het voor de werkbaarheid en effectiviteit van de regelgeving van belang dat aan bepaalde randvoorwaarden is voldaan. Daarbij gaat het in de zorg met name om de beschikbaarheid van voldoende gekwalificeerd (ICT) personeel. Hoewel het college erkent dat dit geen direct onderdeel vormt van de ministeriële regeling, is deze randvoorwaarde wel van belang om de beleidsdoelen te behalen.

3.1 Het college adviseert toe te lichten of aan de noodzakelijke randvoorwaarde van voldoende gekwalificeerd personeel in de zorg is voldaan.

De verplichting om de toeleveringsketen te beveiligen zal extra regeldruk opleveren ten opzichte van al bestaande verplichtingen in de zorg. Dit vergt zeker voor kleinere en middelgrote zorgorganisaties veel kennis en capaciteit, zeker om te bepalen om welke leveranciers het precies gaat. Zoals al bij het ATR-advies bij het besluit benoemd, dient er in de uitwerking aandacht te zijn voor de werkbaarheid en lasten voor deze organisaties. De toelichting bij de regeling gaat niet in op hoe zorgorganisaties bij de uitwerking van deze verplichting praktisch worden ondersteund.

3.2 Het college adviseert bij de zorgplicht met betrekking tot de beveiliging van de toeleveringsketen aan te geven hoe (kleinere) zorgorganisaties bij deze verplichting worden ondersteund.

De formulering van de drempelwaarden wanneer een melding dient te worden gedaan, laat volgens de toelichting 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 verstaan wordt onder kritieke bedrijfsmiddelen, kritische bedrijfsprocessen en bedrijfsgevoelige informatie. De drempelwaarden zoals nu geformuleerd in de regeling laten nog veel ruimte voor interpretatie. Zo is onduidelijk welke organisaties in welke situaties allemaal moeten melden. Dit blijkt ook uit diverse internetconsultatiereacties bij het bovenliggende besluit. Bijvoorbeeld als het gaat om de verantwoordelijkheid voor een melding na een storing bij een ICT-leverancier. Moeten alle zorgpartijen van deze leverancier die door een dergelijke storing geraakt worden en daardoor komen te vallen onder de drempelwaarden dit melden? Om onnodige meldingen en bijkomende rapportageverplichtingen (zie ook adviespunten onder toetsvraag 2) of juist non-compliance te voorkomen, acht het college het nodig om met diverse scenario's duidelijkheid te geven over wie eigenaar en verantwoordelijke is voor meldingen in diverse situaties.

3.3 Het college 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.

Bij de wet heeft ATR geadviseerd om na een jaar een (generieke) invoeringstoets uit te voeren. Dit adviespunt is niet opgevolgd: er zal alleen een evaluatie na 4 jaar worden uitgevoerd. Het college acht het van belang dat er alsnog een invoeringstoets plaatsvindt en dan specifiek voor de zorgsector, omdat met een dergelijke invoeringstoets sneller kan worden ingespeeld op mogelijke knelpunten en tijdig kan worden bepaald of de criteria voor significante incidenten en de uitwerking van de zorgplicht passend en werkbaar zijn voor de sector. Niet alle knelpunten zijn immers te voorzien of weg te nemen, zeker gezien de grote diversiteit van organisaties binnen de zorgsector. Met een invoeringstoets kan ook sneller gekeken worden waar lastenvermindering mogelijk is. Een invoeringstoets acht het college tot slot ook passend gezien de snel opeenvolgende technologische ontwikkelingen.

3.4 Het college adviseert na een 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.

Tot slot constateert het college dat de Regeling weerbaarheid kritieke entiteiten zorg (RwkeZ, waarin ook een zorgplicht wordt geregeld) op een later moment wordt geconsulteerd. Andere departementen consulteren deze regelingen wel gelijktijdig. Om de samenhang tussen beide regelingen te borgen is het van belang is dat ook de RwkeZ zo snel mogelijk openbaar geconsulteerd wordt.

4. Gevolgen regeldruk

Algemeen

De toelichting bevat een nadere regeldrukanalyse ten opzichte van wat eerder bij de wet en besluit in beeld is gebracht. De toelichting benoemt dat voor een aanvullende analyse is gekozen omdat 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 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 en sectoren. De uitkomsten van het onderzoek geven een actuele en sectorspecifieke weergave van de te verwachten regeldrukkosten. Het college merkt op dat bij de verschillende onderdelen van de regeldrukanalyse duidelijk moet worden gemaakt of deze geraamde kosten aanvullend zijn op de wet en besluit of een nadere concretisering inhouden.

Het college acht het positief dat de aanvullende analyse is uitgevoerd. Bij de andere sectorale regelingen is een dergelijke aanvullende analyse niet uitgevoerd.[2]

Zorgplicht

De eenmalige regeldrukkosten van de zorgplicht worden geschat op € 54.789.687,-. Een deel van de organisaties verwacht volgens de analyse structureel extra kosten te zullen moeten maken om aan nieuwe werkwijzen te voldoen. Als belangrijkste oorzaak voor deze kosten wordt de extra tijdbesteding voor de beveiliging van de toeleveringsketen genoemd. De structurele regeldrukkosten schatten deze organisaties op € 55.821,- per organisatie. De totale structurele regeldrukkosten van de zorgplicht bedragen € 66.314.839,-.

Het college merkt op dat niet duidelijk is of zogenaamde '*trickle down effecten'* in deze bedragen zijn meegenomen. Toeleveranciers vallen in sommige gevallen zelf niet onder de nieuwe regelgeving, maar moeten wel informatie aanleveren aan belangrijke en essentiële entiteiten zodat deze de informatie als bewijs kunnen overleggen aan een toezichthouder en/of alsnog zelf aanpassingen kunnen doen om (indirect) aan de regelgeving te voldoen. Dit zorgt voor indirecte regeldrukgevolgen.

4.1 Het college adviseert toe te lichten of indirecte kosten (zgn. '*trickle down effecten*') ook in de regeldrukanalyse zijn meegenomen. Als dit niet het geval is, dienen deze kosten alsnog in beeld te worden gebracht.

Meldplicht

Zorgorganisaties 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, variëren tussen organisaties van eenmaal 5 minuten tot 1 FTE gedurende 4 maanden. Deze eenmalige regeldrukkosten worden op € 4.944.382,- geschat.

De structurele regeldrukgevolgen bestaan uit het melden van cyberincidenten. Deze worden op € 13.367.567,- geschat. Het college merkt hierbij op dat onduidelijkheid over verantwoordelijkheden en eigenaarschap van meldingen (zie adviespunt 3.3) tot aanzienlijk meer regeldruk kan leiden. Daarbij is onduidelijk of in de berekeningen is meegenomen of zorgorganisaties meer personeel moeten aannemen om de nieuwe eisen te voldoen.

4.2 Het college adviseert toe te lichten of in de regeldrukberekeningen ook het eventueel aannemen van nieuw personeel is meegenomen. Als dit niet het geval is, is het advies dit alsnog te doen.

[2] In die gevallen geven departementen aan dat de regeldruk bij bovenliggende wetgeving al in beeld is gebracht (en dus geen aanvulling behoeft). Dit is onjuist, want de regeldrukanalyse bij wet en besluit bevatte geen sectorspecifieke uitwerking. Ook miste een analyse van de kosten voor het melden van incidenten.

Dictum

Gelet op bovengenoemde bevindingen is het eindoordeel ten aanzien van dit voorstel:

Niet indienen / vaststellen tenzij met de adviespunten rekening wordt gehouden.

Het college benadrukt dat dit dictum geen inhoudelijk oordeel is over het voorstel maar alleen de onderbouwing ervan betreft. Het voorstel kan minder belastend in de uitwerking en toezicht. Ook is bij de meldplicht en de rapportageverplichtingen sprake van een nationale kop. Verder behoeft de onderbouwing van de werkbaarheid voor kleinere zorgorganisaties op onderdelen nadere toelichting en verduidelijking. De toelichting bevat nog onvoldoende concretisering van abstracte, juridische bepalingen. Tot slot is de regeldrukanalyse nog niet compleet.

Het college vertrouwt erop u hiermee voldoende te hebben geïnformeerd over de uitkomsten van de toetsing. Het gaat ervan uit dat de toelichtingen bij de voorstellen duidelijk zullen maken op welke wijze met de genoemde adviespunten rekening is gehouden. Het college verzoekt u eventueel gewijzigde voorstellen aan ATR voor te leggen, zodat wij kunnen bepalen of aanvullende zienswijzen opportuun zijn.

Hoogachtend,

w.g.

M.A. van Hees
Voorzitter

R.W. van Zijp
Secretaris