Consultatie van het voorontwerp voor de

Cyberbeveiligingswet

Reactie van KPN

KPN
Postbus 25110
3001 HC Rotterdam

28 juni 2024

Inleiding

KPN maakt graag gebruik van de gelegendheid om te reageren op de consultatie van de Cyberbeveiligingswet (hierna "**Cbw**"). KPN is in het algemeen positief ten aanzien van de Europese NIS2-richtlijn en de Nederlandse implementatie in de Cyberbeveiligingswet. De digitale veiligheid, weerbaarheid en harmonisatie in Europa zijn van groot belang voor een weerbaarder Nederland en Europa en voor de continuiteit van de entiteiten in scope.

Gelijktijdig met het indienen van deze consultatiereactie dient KPN ook een consulatiereactie in op de Wet weerbaarheid kritieke entiteiten (hierna: '**Wwke**'). Met betrekking tot de onduidelijkheid over de situaties waarin de Wwke van toepassing is en wanneer de Cbw, is er een overlap in de consultatiereacties.

Er zijn een aantal belangrijke punten waar KPN aandacht voor vraagt in deze consultatiereactie.

- **Inconsistentie wegnemen**: KPN verzoekt geen inconsistentie te laten bestaan tussen de tekst van de Wwke en de toelichting daarop in de Cbw en de Wwke. Dit leidt tot onduidelijkheid tav de toepasbaarheid van de Cbw en de Wwke.
- **Invulling zorgplicht conform NIS2, geen nationale kop**: KPN verzoekt om bij de invulling van de zorgplicht geen aanvullende vereisten op te leggen aan Nederlandse bedrijven, maar aan te sluiten bij de huidige eisen die zijn neergelegd in de NIS2-richtlijn om aldus niet opnieuw verschillen te laten ontstaan tussen de Europese landen.
- **Redelijke invulling van bestuurdersaansprakelijkheid**: KPN verzoekt artikel 26 lid 1 en 2 Cbw zodanig te herschrijven dat hieruit duidelijk volgt dat ieder lid van de Raad van Bestuur een opleiding moet volgen en over voldoende kennis moet beschikken om eindverantwoordelijkheid te kunnen dragen op basis van rapportage van en gesprekken met de specialisten binnen het bedrijf.
- **Verduidelijking artikel 26 tav 'bestuurder':** KPN verzoekt in de Cbw of de toelichting daarop een verduidelijking op te nemen waarbij bij de uitleg van de in artikel 26 Cbw genoemde 'bestuurder' wordt aangesloten bij Boek 2 van het Burgerlijk Wetboek, zodat duidelijk is dat artikel 26 ziet op de algemeen directeur en de overige wettelijke vertegenwoordigers.
- **Meldplicht, aansluiting van huidige drempelwaarden van de Wbni**: KPN verzoekt de Minister om bij de invulling van die term 'significant incient' in artikel 27 Cbw aan te sluiten bij de huidige invulling van deze term onder de Wbni.
- **Geen uitbreiding meldloketten**: KPN verzoekt de Minister om de meldplichten zoveel mogelijk in lijn te brengen met de al bestaande meldplichten die overlap kunnen hebben met de meldplichten beschreven in de Cbw en het aantal verplichte meldloketten zo veel mogelijk te beperken.
- **Maak de handhavingsbepalingen proportioneel:** KPN verzoekt de Minister om de handhavingsbepalingen proportioneel te maken, bijvoorbeeld door in de Cbw op te nemen dat de handhavingsbepalingen genoemd in hoofdstuk 16.2 Cbw, vooraf moeten worden gegaan door een waarschuwing.

- **Geen verruiming van openbaarheid van meldingen**: KPN verzoekt een aanpassing van de wijziging van de bijlage bij de Wet Open Overheid, in lijn met het huidige artikel 11a.2 Tw, waardoor niet alle meldingen automatisch onder de Wet Open Overheid vallen, maar pas openbaar worden indien dat in het algemeen belang is en daartoe is besloten door de Minister.
- **Beleidsneutrale omzetting van de NIS2**: KPN verzoekt de Minister om bij de mogelijkheden in de Cbw voor nadere invulling steeds het doel van de NIS2-richtlijn (harmonisatie) en het gelijke speelveld leidend te laten zijn en geen nationale kop op de wetgeving toe te voegen.

Hieronder zal KPN deze verzoeken nader toelichten.

Eenduidigheid ten aanzien van de toepassing van de Cbw en de Wwke

Cbw en MvT ten aan zien van verhouding tussen de twee nieuwe wetten

Het toepasssingsbereik van de Cbw is vastgelegd in hoofdstuk 3 van het wetsvoorstel Cbw.

In de toelichting bij het wetsvoorstel, paragraaf 2.4, is een nadere duiding van de verhouding van de Cbw tot de CER richtlijn en de Wwke opgenomen. Daarin staat onder andere dat entiteiten op basis van de Cbw maatregelen moeten treffen om de risico's voor netwerk- en informatiesystemen te beheersen voor zowel 1) de digitale beveiliging van die systemen, als 2) de bescherming van de fysieke omgeving en componenten van die systemen, zoals gebouwen en ruimtes waar die systemen zich bevinden. De toelichting stelt daarbij dat indien een incident of bijna-incident gevolgen heeft die zowel de netwerk- en informatiesystemen betreffen als een verstoring van *andere fysieke aspecten die de essentiële dienstverlening raken*, ook de verplichtingen van de Wwke gelden.

Op basis van de toelichting lijkt het verschil te zitten in "*andere fysieke aspecten die de essentiele dienstverlening raken*", niet zijnde de fysieke omgeving of componenen van die systemen. Wat hieronder valt, is nu echter niet duidelijk en kan tot verwarring leiden.

Wwke en MvT ten aanzien van de verhouding tussen de twee nieuwe wetten

In onder andere artikel 15 (risicobeoordeling), artikel 17 (zorgplicht), artikel 19 (meldplicht), artikel 24 (verbindingsfunctionaris) en artikel 27 (entiteiten van Europees belang) van de Wwke is opgenomen dat die genoemde verplichtingen uit de Wwke niet van toepassing zijn op kritieke entiteiten in de sector digitale infrastructuur. KPN vindt dit een goede zaak, omdat zo dubbel werk en onnodige lasten kunnen worden voorkomen.

Volgens de Memorie van Toelichting zijn er echter wél Wwke-verplichtingen van toepassing wanneer er een "*verstoring van andere fysieke aspecten*" plaatsvindt die de essentiële dienstverlening van KPN raakt. Dit is opgenomen in de Memorie van Toelichting op de Wwke op p 6, paragraaf 2.3. Tevens is dit opgenomen in de Memorie van Toelichting op de Cbw, op p. 7, paragraaf 2.4.

Wwke MvT 2.3, p. 6	Cbw MvT 2.4, p. 7
"Het kan wel voorkomen dat een incident of bijna-incident gevolgen heeft die zowel de netwerk- en informatiesystemen en de fysieke omgeving daarvan betreffen, als een verstoring van andere fysieke aspecten die de essentiële dienstverlening raken. In dat geval gelden de verplichtingen van beide wetten. De Cbw beschrijft dan de verplichtingen van de kritieke entiteit en de respons van de bevoegde autoriteit daarop die zich uitstrekt over specifiek de netwerk- en informatiesystemen en de fysieke omgeving daarvan. Voor het overige is dit wetsvoorstel van toepassing."	*"Het kan wel voorkomen dat een incident of bijna-incident gevolgen heeft die zowel de netwerk- en informatiesystemen betreffen als een verstoring van andere fysieke aspecten die de essentiële dienstverlening raken. In dat geval gelden de verplichtingen van beide wetten. De Wwke beschrijft dan de verplichtingen van de kritieke entiteit en de respons van de bevoegde autoriteit daarop, die zich niet uitstrekt over de netwerk- en informatiesystemen of de fysieke omgeving daarvan. Voor die systemen en de omgeving daarvan is de Cbw van toepassing."*

Dit verschil zorgt voor verwarring en onduidelijkheid. Op grond van onderstaande argumenten pleit KPN voor aanpassing van de Memorie van Toelichting en daarmee verduidelijking van de Wwke.

Inconsistentie tussen de Memorie van Toelichting en de wettekst van de Wwke

De toelichting op de Cbw, paragraaf 2.4 is in tegenspraakmet de wettekst van de hierboven genoemde artikelen in de Wwke, waarin is bepaald dat deze niet van toepassing zijn op kritieke entiteiten in de digitale infrastructuursector. Die bepalingen in de wet maken geen voorbehoud voor de "*verstoring van andere fysieke aspecten die de essentiele dienstverlening raken*".

Ontbrekende grondslag in Europese regelgeving

In de Europese regelgeving is aangegeven dat de hoofdstukken III, IV en VI van de CER-richtlijn niet gelden voor de sector digitale infrastructuur. Ten aanzien van deze bepaling is noch in de CER noch in de NIS2 een bepaling opgenomen die de afwijking van deze bepaling, zoals opgenomen in paragraaf 2.4 van de Memorie van Toelichting, ondersteunt. De lidstaten kunnen op grond van artikel 8 van de CER-richtlijn slechts nationale bepalingen vaststellen of handhaven om tot een hoger weerbaarheidsniveau van kritieke entiteiten te komen voor zover die bepalingen stroken met het toepasselijke Unierecht. In dit geval laat de Uniewetgever echter geen beleidsruimte, aangezien de verplichtingen die voortvloeien uit hoofdstukken III, IV en VI van de CER-richtlijn door de Uniewetgever expliciet zijn uitgesloten voor kritieke entiteiten die die deel uitmaken van de sector digitale infrastructuur.

De term "*verstoring van andere fysieke aspecten die de essentiele dienstverlening raken*" is onduidelijk

De uitzondering die is genoemd in de Memorie van Toelichting geldt voor een "*verstoring van andere fysieke aspecten die de essentiële dienstverlening raken"*. Het is onduidelijk wat precies onder deze verstoring valt en welke andere fysieke aspecten worden beoogd hieronder te laten vallen wanneer een dergelijke verstoring de essentiële dienstverlening van KPN raakt. KPN kan hierbij zelf geen voorbeelden voorstellen.

Het zou behulpzaam zijn als een en ander wordt gespecificeerd en/of voorbeelden worden gegeven van ‘de andere fysieke aspecten die de essentiele dienstverlening raken’.

KPN verzoekt om bovenstaande redenen de Memorie van Toelichting, paragraaf 2.4 zodanig aan te passen dat die consistent is met de wettekst van de Wwke en de Europese regelgeving waarop de Wwke is gebaseerd.

KPN verwacht dat bij bovenstaand verzoek de term “*verstoring van andere fysieke aspecten die de essentiële dienstverlening raken”* wordt verwijderd uit de toelichting. Mocht deze term worden gehandhaafd dan verzoekt KPN de Minister om deze term nader toe te lichten, oa met voorbeelden.

Zorgplicht

KPN onderschrijft de voorgenomen implementatie van de invulling van de zorgplicht zoals omschreven in artikel 23 lid 1 en 2 van het wetsvoorstel voor de Cbw. KPN heeft echter wel een kanttekening bij de toelichting bij dit artikel.

Aanvullende vereisten, niet wenselijk gezien ervaring van NIS1 en doel NIS2

KPN is onaangenaam verrast dat in de toelichting onder paragraaf 5.3.5 is opgenomen dat op grond van artikel 23 lid 4 Cwb in een nog op te stellen algemene maatregel van bestuur naar verwachting gebruik zal worden gemaakt van de in de NIS2-richtlijn opgenomen mogelijkheid om maatregelen op te nemen die een hoger beveiligingsniveau voorschrijven aan bedrijven in Nederland dan het beveiligingsniveau dat voor Europa nu is vastgelegd in NIS2.

Dit druist ook in tegen een van de belangrijkste doelen van de NIS2 richtlijn. In overweging 4 en 5 van de NIS2 richtlijn staat immers beschreven dat het gebrek van de NIS1 richtlijn was dat er geen uniforme implementatie was in de diverse Europese landen, met een nadelig effect op de werking van de interne markt. Zie onder andere onderstaande toelichting uit deze overwegingen:

> *“De cyberbeveiligingseisen die worden gesteld aan entiteiten die diensten of economisch belangrijke activiteiten verrichten, verschillen aanzienlijk van lidstaat tot lidstaat wat betreft het soort eisen, de mate van gedetailleerdheid en de wijze van toezicht.”*
>
> *“Die verschillen brengen extra kosten met zich mee en leveren problemen op voor entiteiten die goederen of diensten aanbieden over de grenzen heen. De eisen die door de ene lidstaat worden gesteld en die verschillen van of zelfs in strijd zijn met de door een andere lidstaat gestelde eisen kunnen een aanzienlijke invloed hebben op deze grensoverschrijdende activiteiten.”*
>
> *“Al deze verschillen leiden tot een versnippering van de interne markt en kunnen een nadelig effect hebben op de werking ervan, wat met name gevolgen heeft voor de grensoverschrijdende dienstverlening en het niveau van de digitale weerbaarheid als*

gevolg van de toepassing van diverse maatregelen. Uiteindelijk kunnen die verschillen sommige lidstaten uiteindelijk meer kwetsbaar maken voor cyberdreigingen, met mogelijke overloopeffecten in de hele Unie."

KPN is dan ook van mening dat het opnemen van zwaardere maatregelen in de Nederlandse wet dan die neergelegd in de NIS2-richtlijn, niet wenselijk is en in strijd met het doel van Europese harmonisatie. Bovendien leidt dit aantoonbaar tot lastige discussies met andere internationale partijen, waaronder leveranciers.

KPN verzoekt om geen aanvullende vereisten op te leggen aan Nederlandse bedrijven, maar aan te sluiten bij de huidige eisen die zijn neergelegd in de NIS2-richtlijn en op die manier niet opnieuw verschillen te laten ontstaan tussen de Europese landen.

Redelijke invulling bestuurdersaansprakelijkheid

In het voorstel voor de Cbw is opgenomen dat het bestuur van een entiteit wordt geacht in staat te zijn toe te zien op de cyberbeveiligingsbeheersmaatregelen en de uitvoering en de beoordeling hiervan; zie het voorgestelde artikel 26 lid 1 Cbw en het daarmee corresponderende artikel 20 van de NIS2-richtlijn. Oftewel, het bestuur is eindverantwoordelijk voor de cyberbeveiligingsbeheersmaatregelen en ziet erop toe dat deze worden uitgevoerd, maar zij voeren deze zelf niet uit. Het bestuur moet door het regelmatig volgen van een opleiding zorgen voor voldoende kennis om de eindverantwoordelijkheid te kunnen dragen op basis van rapportage van en gesprekken met de specialisten binnen het bedrijf.

In het tweede lid van artikel 26 van het wetsvoorstel staat echter dat het bestuur ook geacht wordt om over de benodigde kennis en vaardigheden te beschikken om risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren en beoordelen, alsmede de gevolgen daarvan voor de diensten. Deze interpretatie van de NIS2-richtlijn is echter niet praktisch uitvoerbaar en zou drastisch afwijken van de gangbare regimes omtrent oa kennis die verondersteld wordt van bestuurders met betrekking tot financien. Het identificeren van risico's en in eerste instantie beoordelen van risicobeheersmaatregelen en de gevolgen daarvan, zijn taken die binnen een entiteit door speciaal daarvoor (hoog) opgeleide en ervaren medewerkers worden uitgevoerd. De bestuurders moeten zodanig worden opgeleid dat ze over voldoende kennis beschikken om eindverantwoordelijkheid te kunnen dragen op basis van rapportage van en gesprkken met specialisten binnen het bedrijf. Artikel 26 lid 2 van het wetsvoorstel dient daarmee in lijn te worden aangepast.

KPN verzoekt artikel 26 lid 1 en 2 Cbw zodanig te herschrijven dat hieruit duidelijk volgt dat ieder lid van de Raad van Bestuur een opleiding moet volgen en over voldoende kennis moet beschikken om eindverantwoordelijkheid te kunnen dragen op basis van rapportage van en gesprekken met de specialisten binnen het bedrijf.

Verduidelijking artikel 26 Cbw

KPN leest artikel 26 Cbw zo dat onder bestuur het bestuur wordt verstaan in de zin van Boek 2 van het Burgerlijk Wetboek (BW); het bestuur bestaat uit de personen die zijn belast met het besturen van de vennootschap, oftewel de algemeen directeur en de overige wettelijke vertegenwoordigers. De Raad van Commissarissen heeft tot taak toezicht te houden op het beleid van het bestuur en op de algemene gang van zaken in de vennootschap en de met haar verbonden onderneming (ook Boek 2 BW). De leden van de Raad van Commissarissen vallen daarmee niet onder het bestuur van de vennootschap. Om misverstanden te voorkomen, verzoekt KPN dit te verduidelijken in de wet of de toelichting daarop.

KPN verzoekt in de Cbw of de toelichting daarop een verduidelijking op te nemen omtrent de in artikel 26 Cbw genoemde 'bestuurder', waarbij bij de uitleg wordt aangesloten bij Boek 2 van het Burgerlijk Wetboek, zodat duidelijk is dat artikel 26 Cbw ziet op de algemeen directeur en de overige wettelijke vertegenwoordigers.

Meldplicht

Aansluiten bij drempelwaarden van de Wbni

In de toelichting, paragraaf 5.5.1, is aangegeven dat op basis van de tekst van het voorgestelde artikel 37 van de Cbw in een algemene maatregel van bestuur nadere regels zullen worden gesteld met betrekking tot de invulling van de term 'significant incident' van het voorgestelde artikel 27.

Deze nadere regels zijn bepalend voor de last, de uitvoerbaarheid en de efficiëntie van de op grond van de NIS2-richtlijn te implementeren meldplicht. De last ziet vooral op de administratieve last voor de bedrijven die de meldingen moeten doen, inclusief updates, tussentijdse verslagen, voortgangsverslag en eindverslag. Gelijk daarmee loopt natuurlijk de administratieve last voor het meldpunt. De uitvoerbaarheid houdt mede verband met het voorgestelde artikel 27 lid 2 dat ook een 'kan'-bepaling omvat (het gaat niet langer om verstoringen die daadwerkelijk de genoemde gevolgen hebben, maar ook om verstoringen die dat *kunnen* hebben), waardoor, indien de drempelwaarde niet zorgvuldig wordt gekozen, het meldpunt overspoeld kan worden door meldingen van de betreffende entiteiten, hetgeen een enorme uitvoeringslast en verlaging van efficiëntie met zich mee kan brengen.

KPN pleit dan ook voor een proportionele, risicogebaseerde drempelwaarde voor de meldplicht. Focus moet liggen op continuïteit van de essentiële of belangrijke dienstverlening. Het wettelijk melden moet gericht zijn en blijven op de (mogelijke) continuïteitssituaties. Voor een algemeen beeld en inzicht in hetgeen waar entiteiten mee geconfronteerd worden op het gebied van mogelijke aanvallen, kwetsbaarheden etc. kan gebruik worden gemaakt van informatie die gedeeld wordt in oa de sectorale ISAC's waar het NCSC aan deelneemt.

Onder de huidige Wbni zijn ook drempelwaarden bepaald voor de meldingen op grond van die wet. Deze drempelwaarden worden door KPN gesteund.

KPN verzoekt de Minister om bij de invulling van die term ‘significant incident’ in artikel 27 Cbw aan te sluiten bij de huidige invulling van deze term onder de Wbni.

Geen uitbreiding van meldloketten

Met de komst van de Cbw naast de al bestaande wetten waarin een meldplicht is opgenomen, zoals de AVG en toekomstige wetten zoals de CRA, is het aannemelijk dat bij één incident meldingen moeten worden gedaan bij meerdere toezichthouders, én bij de CSIRTs én bij ENISA. Dit komt de focus op het nemen van mitigerende maatregelen bij een beveiligingsincident niet ten goed en zorgt voor extra administratieve lasten bij zowel de melder als de toezichthoudende instanties, CSIRT’s en ENISA.

KPN verzoekt de Minister om de meldplichten zoveel mogelijk in lijn te brengen met de al bestaande meldplichten die overlap kunnen hebben met de meldplichten beschreven in de Cbw en het aantal verplichte meldloketten zo veel mogelijk te beperken.

Maak de handhavingsbepalingen proportioneel

Voor essentiële entiteiten zijn een groot aantal handhavingsbepalingen opgenomen die grote consequenties kunnen hebben, waaronder het verplicht door een onafhankelijke deskundige laten uitvoeren van een beveiligingsscan, een gerichte beveiligingsaudit en/of een ad hoc beveiligingsaudit. Daarbij is tevens bepaald dat de kosten van dergelijke audits voor rekening komen van de essentiële entiteit. Er is echter geen proportionaliteitstoets in deze bepalingen opgenomen, waardoor in principe elke entiteit op ieder moment een dergelijke verplichting opgelegd kan krijgen met de daarbij behorende kosten.

Doordat de genoemde bepalingen geen vooraf gedefinieerde trigger hebben, zoals een waarschuwing, kan dit door de toezichthouder aangegrepen worden om de hierboven beschreven activiteiten uit te voeren als vervanging van toezicht door de toezichthouder. Hierdoor komen de kosten van het toezicht, bestaande uit commerciële tarieven van consultancy en beveiligingsbedrijven volledig voor rekening van de entiteit, zonder dat de entiteit daar invloed op uit kan oefenen.

Ook in de andere handhavingsbepalingen, zoals het geven van een bindende aanwijzing en een last onder dwangsom is geen volgordelijkheid aangegeven, dan wel aangegeven dat deze vooraf worden gegaan door een waarschuwing. Het zou logisch zijn als een essentiele entiteit bij een (vermoeden van) overtreding van een bepaling uit de Cbw eerst een waarschuwing krijgt alvorens de overige vergaande handhavingmaatregelen worden ingezet, die zeer arbeidsintensief kunnen zijn voor de essentiële entiteit en bovendien veel kosten met zich mee kunnen brengen.

KPN verzoekt de Minister om de handhavingsbepalingen proportioneel te maken, bijvoorbeeld door in de Cbw op te nemen dat de handhavingsbepalingen genoemd in hoofdstuk 16.2 Cbw, vooraf moeten worden gegaan door een waarschuwing.

Geen verruiming van openbaarheid van meldingen

Parallelle toepassing van het huidige artikel 11a.2 lid 3 Tw

In het voorgestelde artikel 90 Cbw is een grote wijziging opgenomen die onwenselijk is en niet bijdraagt aan de veiligheid van Nederland. Dit artikel wijzigt namelijk de bijlage bij artikel 8.8 van de Wet Open Overheid (WOO). In deze bijlagen staan de uitzonderingen voor openbaarmaking opgesomd, daaronder valt onder de huidige bijlage ook de Telecommunicatiewet. In de huidige Telecommunicatiewet staat onder andere:

> *"1. Aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten stellen Onze Minister onverwijld in kennis van beveiligingsincidenten met aanzienlijke gevolgen voor het functioneren van hun netwerken of diensten.*
>
> *2. Aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten verstrekken onze Minister op zijn verzoek alle informatie die nodig is om de beveiliging van hun netwerken of diensten te beoordelen.*
>
> *3. Op grond van het eerste en tweede lid verstrekte gegevens zijn niet openbaar. Indien openbaarmaking in het algemeen belang is, kan Onze Minister een inbreuk op de veiligheid en een verlies van integriteit, bedoeld in het eerste lid, openbaar maken of de aanbieder verplichten tot openbaarmaking."* Artikel 11a.2 lid 1-3 Tw

Uit deze huidige bepalingen volgt dat beveiligingsincidenten en informatie die wordt verstrekt om de beveliging van de netwerken of diensten van telecompartijen te beoordelen, niet op elk moment door een ieder op te vragen is, maar slechts indien dat in het algemeen belang is en na een formeel besluit van de Minister.

Door de invoering van het voorgestelde artikel 90 Cbw zou deze uitzondering op de openbaarmaking op grond van de Woo komen te vervallen. Deze uitzondering wordt slechts vervangen door een uitzondering voor communicatie tussen het CSIRT en de overheid.

Het potentieel openbaar worden van meldingen, zoals nu omschreven in artikel 90 Cbw, komt niet ten goede aan de veiligheid van Nederland in het algemeen; een eventuele openbaarmaking zal steeds zorgvuldig moeten worden afgewogen op grond van een speciaal daarvoor bedoelde wettelijke bevoegheid. KPN pleit daarom voor een aanpassing van artikel 90 Cbw waarbij de lijn van het huidige artikel 11a.2 Tw wordt gevolgd; slechts verstrekking van informatie over meldingen die zijn gedaan indien dit in het algemeen belang is en na een formeel besluit van de relevante minister.

KPN verzoekt artikel 90 Cbw aan te passen in lijn met het huidige artikel 11a.2 Tw.

Beleidsneutrale omzetting NIS2 richtlijn

In de Cbw is een redelijk groot aantal mogelijkheden opgenomen om bij algemene maatregel van bestuur nadere regels te stellen. Omwille van een gelijk speelveld in Europa is KPN voorstander van een beleidsneutrale omzetting van de NIS2-richtlijn in de nationale wet- en regelgeving. Zoals hierboven al opgemerkt, wordt KPN hierin gesterkt door de overwegingen van de NIS2-richtlijn.

KPN verzoekt de Minister om bij de mogelijkheden in de Cbw voor nadere invulling steeds het doel van de NIS2-richtlijn en het gelijke speelveld leidend te laten zijn.