Beleidskompasformulier voor **internetconsultatie**

Instructie voor gebruik:

Dit is het formulier voor de beantwoording van de Beleidskompasvragen ten behoeve van internetconsultatie. Per 29 maart 2023 worden bij nieuwe internetconsultaties de antwoorden op de vragen van het Beleidskompas gepubliceerd. Let op dat dit formulier op enkele punten afwijkt van het reguliere Beleidskompasformulier, aangezien dit formulier terugblikt op de stappen voorafgaand aan de consultatie.

Alle tekstvakken in het formulier dienen te worden ingevuld en vragen mogen niet worden verwijderd. Indien het voorstel een technische wijziging betreft of om een andere reden beleidsarm is, kan bij de vragen die niet van toepassing zijn worden volstaan met het invullen van "n.v.t.".

Verwijder de cursief gedrukte tekst na beantwoording van de vragen.

Titel:

Regeling cyberbeveiliging LVVN

∞ Wie zijn belanghebbenden en waarom?

Toelichting

Hulpvragen

- Wie zijn direct of indirect belanghebbenden bij het betreffende vraagstuk?

Het Ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur en het Ministerie van Justitie en Veiligheid zijn direct belanghebbend. Indirect belanghebbend zijn het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, het Ministerie van Economische Zaken, het Ministerie van Klimaat en Groene Groei, het Ministerie van Financiën, het Ministerie van Infrastructuur en Waterstaat, het Ministerie van Onderwijs, Cultuur en Wetenschap, het Ministerie van Defensie en het Ministerie van Volksgezondheid, Welzijn en Sport. De entiteiten uit de levensmiddelenindustrie die onder het toepassingsbereik van de Cyberbeveiligingswet komen te vallen en brancheorganisaties. De bevoegde autoriteiten die toezicht zullen houden op de naleving van de verplichtingen uit de Cyberbeveiligingswet. Voor de levensmiddelenindustrie is dit de Nederlandse Voedsel- en Warenautoriteit (NVWA). De computer security incident response teams (CSIRT's) die ondersteuning zullen leveren aan entiteiten. Voor de levensmiddelenindustrie is dit het National Cyber Security Centrum.

- Wie beschikken er over relevante kennis over en ervaring met het vraagstuk?

Zie voorgaand.

- Op welke wijze zijn belanghebbenden tot nu toe in de verschillende fasen van het beleidstraject betrokken?

Belanghebbenden zijn betrokken geweest bij de voorbereidingen van de ministeriële regeling.

1. Wat is het probleem?

Toelichting

Hulpvragen

a) Wat is het probleem?

De NIS2-richtlijn (Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148, PbEU 2022, L 333) beoogt een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie te bereiken, teneinde de werking van de interne markt te verbeteren. In Nederland wordt de NIS2-richtlijn geïmplementeerd in de Cyberbeveiligingswet. Veel bepalingen zijn omgezet in deze wet en het onderliggende Cyberbeveiligingsbesluit (amvb). Ten behoeve van de nationale implementatie van de richtlijn, is nadere sectorale invulling van een aantal van deze bepalingen nodig. Deze regeling geeft deze nadere sectorale invulling voor de levensmiddelensector.

b) Wat zijn de oorzaken van het probleem?

De NIS2-richtlijn geldt voor een uiteenlopend aantal sectoren en publieke processen met elk hun eigen kenmerken en soort aanbieders.

c) Wat is de omvang van het probleem?

Zie vraag 1a.

d) Wat is het huidige beleid en wat heeft de evaluatie opgeleverd?

De NIS2-richtlijn is tot stand gekomen mede naar aanleiding van een evaluatie van de NIS1-richtlijn. Uit deze evaluatie bleek bijvoorbeeld dat lidstaten de richtlijn op verschillende manieren interpreteerden. Deze verschillen tussen lidstaten leiden tot een versnippering van de interne markt en kunnen een nadelig effect hebben op het functioneren van de interne markt, met gevolgen voor onder meer de grensoverschrijdende dienstverlening.

De NIS2-richtlijn bevat maatregelen om de cyberbeveiliging van essentiële en belangrijke entiteiten binnen de Europese Unie naar een hoger gemeenschappelijk niveau te brengen. De NIS2-richtlijn bevat een lijst van sectoren die binnen reikwijdte vallen. Waaronder de levensmiddelenindustrie. Deze sector viel niet onder reikwijdte van de NIS1-richtlijn.

De NIS2-richtlijn wordt in Nederland geïmplementeerd in de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit (Amvb).

e) Wat gebeurt er als de overheid niets doet (Nuloptie)? Wat rechtvaardigt overheidsinterventie?

Nederland is verplicht om richtlijnen van de Europese Unie te implementeren. In dit geval is overheidsoptreden gerechtvaardigd omdat een publiek belang bestaat, namelijk het waarborgen van de levering van essentiële diensten in de interne markt, waaronder de levering van levensmiddelen.

2. Wat is het beoogde doel?

Toelichting

Hulpvragen

a) Wat zijn de beleidsdoelen?

De NIS2-richtlijn beoogt een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie te bereiken, teneinde de werking van de interne markt te verbeteren. Deze richtlijn beoogt dit doel te bereiken door de verschillen weg te nemen die tussen lidstaten bestaan op het gebied van de cyberbeveiligingseisen die worden gesteld aan entiteiten die economisch belangrijke activiteiten of diensten verrichten. De richtlijn tracht dit doel te bereiken door onder meer regels vast te stellen over entiteiten die van rechtswege, zonder tussenkomst van een lidstaat, onder het toepassingsbereik van de richtlijn komen te vallen, en door te voorzien in doeltreffende voorzieningen ten aanzien van de cyberbeveiligingseisen waar entiteiten aan moeten voldoen en het toezicht op de naleving van de verplichtingen die voortvloeien uit de richtlijn.

In aanvulling op de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit, biedt de onderhavige Regeling cyberbeveiliging levensmiddelensector een nadere sectorale invulling voor de levensmiddelensector.

b) Aan welke duurzame ontwikkelingsdoelen (sustainable development goals, SDG's) en brede welvaartsuitkomsten dragen de doelen bij?

SDG 2

3. Wat zijn opties om het doel te realiseren?

Toelichting

Hulpvragen

a) Wat zijn kansrijke aangrijpingspunten om het doel te realiseren?

De Cyberbeveiligingswet, het Cyberbeveiligingsbesluit en onderliggende regelgeving zorgen voor een wettelijke verankering die aansluit op de doelen die zijn gesteld in de Cybersecuritystrategie 2022-2028. Het doel wordt bereikt door onder meer plichten op te leggen aan entiteiten, zoals de verplichting tot het treffen van adequate ICT-maatregelen en het melden van ICT-incidenten. Naast plichten zijn er ook rechten, zoals het recht op bijstand.

b) Wat zijn, gegeven de aangrijpingspunten, kansrijke beleidsopties?

Zie 3a.

c) Wat is de beleidstheorie (doelenboom) per kansrijke beleidsoptie?

N.v.t.

4. Wat zijn de gevolgen van de opties?

Toelichting

Hulpvragen

a) Wat zijn de verwachte gevolgen per beleidsoptie?

Een verhoogde digitale weerbaarheid van de levensmiddelensector.

Er ontstaan regeldrukeffecten voor de entiteiten die onder het toepassingsbereik van deze implementatiewet- en regelgeving komen te vallen. Zij moeten investeringen doen en inspanningen verrichten om te voldoen aan de verplichtingen die daaruit voortvloeien.

Voor de bevoegde autoriteiten zijn er toezichts- en handhavingskosten.

Voor het Computer security incident response teams (CSIRT), het Nationaal Cyber Security Centrum, zijn er uitvoeringseffecten en -kosten.

b) Welke verplichte toetsen zijn van toepassing en wat zijn daarvan de uitkomsten (voor zover bekend)?

Administratieve lastentoets / regeldrukkosten (Adviescollege toetsing regeldruk)

5. Wat is de voorkeursoptie?

Toelichting

Hulpvragen

a) Wat is het voorstel?

Nederland moet de NIS2-richtlijn implementeren. Voor veel bepalingen uit de richtlijn geschiedt dat middels de Cyberbeveiligingswet en in de algemene maatregel van bestuur (Cyberbeveiligingsbesluit). In onderhavige Regeling cyberbeveiliging levensmiddelensector worden deze sectoraal verder uitgewerkt, onder meer met een uitwerking van de maatregelen die moeten worden genomen in het kader van de zorgplicht en wanneer er sprake is van een significant incident en daarmee een incident voor de levensmiddelensector meldplichtig is.

b) Hoe houdt het voorstel rekening met:

- doeltreffendheid en doelmatigheid;
- uitvoerbaarheid voor alle relevante partijen (inclusief doenvermogen, regeldruk en handhaving);
- brede maatschappelijke impact?

Ja

c) Wat zijn de risico's en onzekerheden van dit voorstel?

n.v.t.

d) Hoe ziet de voorgenomen monitoring en evaluatie eruit?

n.v.t.