Regels ter bevordering van de digitale weerbaarheid van bedrijven (Wet bevordering digitale weerbaarheid bedrijven)

MEMORIE VAN TOELICHTING

A. Algemeen

1. Inleiding

Dit wetsvoorstel regelt de taken en bevoegdheden van de Minister van Economische Zaken en Klimaat (hierna: Minister van EZK) op het gebied van de verbetering van de digitale weerbaarheid van het niet-vitale bedrijfsleven in Nederland. Binnen het ministerie van Economische Zaken en Klimaat (hierna: het ministerie van EZK) is om dit doel te bewerkstelligen, in overeenstemming met de motie Hijink/Tellegen[1], in 2017 het Digital Trust Center (hierna: DTC) opgericht. Aanleiding voor deze motie was de kamerbrede behoefte aan een centrum dat "bedrijven en maatschappelijke organisaties kan informeren en adviseren over én concrete hulp en ondersteuning kan bieden bij het verbeteren van hun cybersecurity en bij het afslaan van aanvallen door hackers". Deze behoefte heeft zijn oorsprong onder meer in het besef dat de kansen van digitalisering alleen optimaal kunnen worden benut wanneer de digitale veiligheid op orde is. Zo niet dan kan zelfs het voortbestaan van een bedrijf in gevaar komen en de Nederlandse concurrentiepositie verzwakken. Het DTC heeft dan ook als missie bedrijven weerbaarder te maken tegen cyberdreigingen. Hiertoe zijn twee hoofdtaken geformuleerd. Ten eerste informatie en advies geven. Ten tweede samenwerking tussen bedrijven op het gebied van digitale weerbaarheid bevorderen. Het DTC is onderdeel van de Directie Digitale Economie (DDE), vallend binnen het Directoraat Generaal Bedrijfsleven en Innovatie (DGB&I) binnen het ministerie van EZK.

Vanuit het DTC wordt nu voornamelijk algemene informatie over digitale dreigingen en incidenten aan het niet-vitale bedrijfsleven gegeven. Er is echter ook behoefte om het bedrijfsleven over specifieke digitale dreigingen en kwetsbaarheden te informeren. Verwacht mag worden dat bedrijven bij een voor hen concrete bedreiging eerder actief zullen worden waar dit nu nog uit blijft bij een meer generieke waarschuwing. Ook zal bij informatie over een specifieke dreiging door het DTC een zo praktisch mogelijk handelingsperspectief worden aangereikt zodat het bedrijf ook weet welke vervolgstap(pen) het kan nemen. Deze uitbreiding van de informatievoorziening vraagt een verdere inbedding van het DTC. Met dit wetsvoorstel worden de taken van het DTC alsook de daaraan gekoppelde bevoegdheid van een formele wettelijke grondslag voorzien. Naast de taken op het gebied van het verstrekken van algemene informatie en stimuleren van samenwerking, omvat dit ook de taak voor het delen van specifieke dreigingsinformatie. In het laatste geval kan het voorkomen dat het DTC

[1] Kamerstukken II 2016/17, 26 643, nr. 474.

bij het ontvangen, verwerken en delen van (dreigings)informatie, persoonsgegevens verwerkt. Door te voorzien in een formele wettelijke grondslag voor de taken en de daaraan gekoppelde bevoegdheden ontstaat tevens een expliciete wettelijke grondslag voor het DTC om in het kader van de taakuitvoering persoonsgegevens te verwerken.

Met dit wetsvoorstel ontstaat er, naast de reeds bestaande bevoegdheden op grond van de Wet beveiliging netwerk en informatiesystemen (Wbni), een nieuwe wettelijke taak voor de Minister van EZK (ingevolge de huidige portefeuilleverdeling de Staatssecretaris).

2. Hoofdlijnen van het voorstel

2.1 Aanleiding

Uit jaarlijks onderzoek van het Centraal Bureau voor de Statistiek (CBS) [2] blijkt dat digitalisering ver is doorgedrongen in het Nederlandse bedrijfsleven. Echter de digitale weerbaarheid van diezelfde bedrijven is nog geen vanzelfsprekendheid. De cijfers tonen aan dat digitalisering en de daaraan gekoppelde weerbaarheid niet alleen afhankelijk zijn de omvang van het bedrijf. Zo zijn er voorbeelden in het grootbedrijf, bij het mkb en zzp'ers, waaruit blijkt dat zij de digitale weerbaarheid op orde hebben. Echter uit onderzoek van het CBS blijkt dat bedrijven, ondanks hun omvang toch slachtoffer blijven van digitale verstoringen en aanvallen[3]. Met de verder doordringende digitalisering wordt de potentiële schade aan het bedrijfsleven, bij het achterblijven van digitale veiligheid en beveiliging, steeds groter. Digitalisering creëert ook nieuwe onderlinge afhankelijkheden bij bedrijven, niet alleen tussen digitale systemen, maar ook in de (digitale) (leveranciers)keten. Het belang van digitale veiligheid en beveiliging groeit omdat de (on)veiligheid van het ene bedrijf, via deze verbindingen invloed kan hebben op de (on)veiligheid eerder of verderop in de keten.

Via het CIO-platform hebben bedrijven via een brief aan de Minister van Justitie en Veiligheid (hierna: de Minister van JenV) [4] gevraagd om te zorgen voor informatiedeling vanuit de overheid met bedrijven als de overheid beschikt over relevante informatie over dreigingen, kwetsbaarheden en incidenten. Op dit moment informeert de overheid door middel van de bestaande structuren, op basis van de Wbni, zowel de rijksoverheid als specifieke doelgroepen binnen het Nederlandse bedrijfsleven, zijnde de vitale bedrijven en digitale dienstverleners. Overige bedrijven kunnen op basis van deze nieuwe grondslag informatie van de overheid ontvangen, dit laat onverlet dat zij eventueel ook informatie via een andere schakelorganisatie als bedoeld in artikel 3, tweede lid, Wbni, zouden kunnen ontvangen. Door deze informatie te verstrekken aan het niet-vitale bedrijfsleven stelt de overheid deze bedrijven

[2] https://longreads.cbs.nl/ict-kennis-en-economie-2020/ict-gebruik-bij-bedrijven/
[3] https://www.cbs.nl/nl-nl/publicatie/2019/37/cybersecuritymonitor-2019
[4] https://www.cio-platform.nl/k/nl/n626/news/view/10130/6631/brief-aan-minister-grapperhaus-versterking-van-de-nederlandse-cyberweerbaarheid.html

in staat om op basis van deze objectieve informatie zelf te beoordelen of en in welke mate zij maatregelen moet treffen ter mitigatie van een kwetsbaarheid, ter afwering van een dreiging of ter oplossing van een daadwerkelijk inbreuk.

De digitale weerbaarheid van bedrijven heeft zowel een economisch effect als een breder maatschappelijk effect doordat bedrijven in verbinding staan met burgers en overheidsorganisaties. Het vergroten van de digitale weerbaarheid van bedrijven levert een belangrijke bijdrage aan de Nederlandse economie. Weerbare bedrijven, dat wil zeggen bedrijven die bewuste, op risico's gebaseerde, keuzes maken over te nemen maatregelen op het gebied van digitale beveiliging, zullen over het algemeen minder snel slachtoffer zijn van digitale verstoringen. Deze maatregelen zijn pluriform. Zo kunnen bedrijven maatregelen nemen op het gebied van awareness, door bijvoorbeeld trainingen voor personeel, specifieke IT-beveiligingsmaatregelen, maar ook maatregelen ten behoeve van de bedrijfscontinuïteit of de inhuur van gespecialiseerde diensten. Afgewogen maatregelen zullen enerzijds een bescherming bieden tegen onbewuste verstoringen anderzijds tegen moedwillige aanvallen. Door afgewogen maatregelen te nemen zullen bedrijven en ondernemers bij een digitaal incident sneller terug kunnen keren naar hun reguliere bedrijfsvoering wat direct bijdraagt aan het verdienvermogen van het bedrijf.

Dit beeld wordt ondersteund door het rapport van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) 'Voorbereiden op digitale ontwrichting'[5] en is tevens benoemd door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in het Cyber Security Beeld Nederland 2020 (CSBN 2020)[6]. In beide rapporten wordt de verregaande digitalisering en de daaraan gerelateerde risico's voor de Nederlandse samenleving benoemd. Door het informeren en adviseren van bedrijven in zijn algemeenheid en specifiek over kwetsbaarheden en dreigingen wordt gewerkt aan een weerbaar bedrijfsleven. Ook de Cyber Security Raad (CSR) adviseert de overheid om, indien zij beschikt over acute dreigingsinformatie die relevant is voor organisaties in Nederland, deze informatie actief te delen met potentiële en daadwerkelijke slachtoffers[7]. Dit wordt ook nog eens bevestigd door het onderzoeksrapport 'Informatie-uitwisseling landelijk dekkend stelsel cybersecurity' uitgevoerd door Dialogic in opdracht van het WODC[8]. een centrale rol in de informatievoorziening aan ondernemend Nederland over digitale weerbaarheid.

[5] WRR-rapport nr. 101, 2019: https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting
[6] https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020
[7] https://cybersecurityraad.nl/010_Actueel/aanscherping-en-uitbreiding-van-maatregelen-noodzakelijk-voor-een-cyberweerbare-samenleving.aspx
[8] https://wodc.nl/wodc-nieuws-2020/cybersecurity-stelsel.aspx

2.2 Wettelijke grondslag voor taken en gegevensverwerking Minister van EZK

De Minister van EZK is beleidsverantwoordelijke voor de bevordering van de digitalisering van ondernemers en heeft al stappen ondernomen om de digitale weerbaarheid van het niet-vitale bedrijfsleven te vergroten. Ten behoeve van de versteviging van de deze rol voorziet dit wetsvoorstel in een vastlegging van de taken van de Minister van EZK op het terrein van digitale weerbaarheid van het niet vitale bedrijfsleven, zoals het verwerken en verspreiden van informatie over kwetsbaarheden, dreigingen en incidenten en het samenwerken met andere bestuursorganen en organisaties (artikel 2). In het kader van deze taakuitoefening mogen persoonsgegevens worden verwerkt.

Voorts voorziet dit wetsvoorstel in een wettelijke grondslag om bijvoorbeeld bij andere publiekrechtelijke organisaties de voor bovengenoemde taakuitoefening noodzakelijke gegevens te vragen en in de mogelijkheid van die derden om in reactie daarop zo nodig ook persoonsgegevens te verstrekken aan de Minister van EZK (artikel 3). Ook voorziet dit wetsvoorstel in de voorwaarden waaronder vertrouwelijke gegevens die bij de Minister van EZK, verstrekt mogen worden aan derden (artikel 4). Ten slotte regelt dit wetsvoorstel een rechtstreekse informatie-uitwisseling tussen overheidsorganisaties die zich met digitale beveiliging bezighouden (artikel, 2, 4 en 5).

Het belangrijkste doel is de versterking van de digitale weerbaarheid van bedrijven (zie de aanhef van artikel 2, eerste lid). Ten behoeve van dat doel heeft de Minister van EZK verschillende taken. Het gaat hierbij allereerst om het analyseren en het onderzoeken van gegevens over kwetsbaarheden, dreigingen en incidenten met betrekking tot netwerk- en informatiesystemen van bedrijven, het informeren en adviseren van bedrijven over voor hun bedrijven relevante kwetsbaarheden, dreigingen en incidenten, én om het verstrekken van informatie over kwetsbaarheden, dreigingen en incidenten gerelateerd aan individuele bedrijven. Deze taken zijn vastgelegd in artikel 2, eerste lid. Op deze manier wordt het mogelijk om specifieke informatie en advies te verwerken en te delen binnen en buiten de overheid. Deze informatie wordt kosteloos aangeboden.

De taken van de Minister van EZK bestaan enerzijds uit het verstrekken van informatie en advies, direct of via samenwerkingsverbanden en anderzijds het verstrekken van actuele digitale dreigingsinformatie en vertrouwelijke informatie ten behoeve van de digitale weerbaarheid van Nederlandse bedrijven aan bedrijven en intermediaire organisaties. In deze zijn intermediaire organisaties vertegenwoordigers van een bepaalde groep aan bedrijven. Denk hierbij aan sector en brancheorganisaties, regionale samenwerkingsverbanden, maar ook sector overstijgende belangenbehartigers van ondernemend Nederland.

Daarnaast heeft de Minister van EZK als taak om de ontwikkeling van samenwerkingsverbanden tussen bedrijven op het gebied van digitale weerbaarheid te stimuleren, samen te werken met

bestuursorganen en rechtspersonen, én om indien relevant de in het kader van analyses en onderzoeken verkregen gegevens aan de Minister van JenV, ten behoeve van de taken van de laatstgenoemde minister, bedoeld in artikel 3, eerste lid, van de Wbni en aan het CSIRT voor digitale diensten, te verstrekken (artikel 2, tweede lid).

De Wbni bevat de taken en bevoegdheden van de Minister van JenV op het terrein van cybersecurity, die in de praktijk worden uitgevoerd door het NCSC. Artikel 3, eerste lid, van die wet regelt als primaire taak van de Minister van JenV de verlening van bijstand bij digitale dreigingen en incidenten aan vitale aanbieders en andere aanbieders die onderdeel zijn van de rijksoverheid. Ook is de Minister van JenV belast met de taak van CSIRT voor een categorie vitale aanbieders (aanbieders van essentiële diensten). Daarnaast regelt artikel 3, tweede lid, van de Wbni dat dreigings- en incidentinformatie met betrekking tot netwerk- en informatiesystemen van andere aanbieders, die in het kader van de primaire taakuitoefening is verkregen, door de Minister van JenV kan worden verstrekt aan de in dat lid bedoelde schakelorganisaties (zoals CSIRT's, computercrisisteams, en organisaties die 'objectief kenbaar tot taak' (OKTT) hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten). Daarnaast voorziet de Wbni ook in de regeling van een CSIRT voor digitale diensten. Deze laatste bevoegdheid is reeds toegekend aan de Minister van EZK.

Met de vorming van de in dit wetsvoorstel opgenomen grondslag ontstaat er de taak en de bevoegdheid voor de Minister van EZK om de voormelde (vertrouwelijke) informatie en adviezen, kwetsbaarheden en dreigingen te verwerken en te delen. Daarbij wordt naast het bestaande regime van de Wbni voorzien in taken en bevoegdheden voor de Minister van EZK, die aldus een plaats krijgt naast de Minister van JenV en krachtens de Wbni als zodanig aangewezen computercrisisteams, CSIRT's en OKTT's, waarmee het stelsel van (overheids)organisaties met een rol in de digitale weerbaarheid van Nederland verder wordt bevorderd.

In de artikelen 3, tweede lid, en 20, tweede lid, van de Wbni zijn organisaties genoemd waarmee het NCSC de in deze artikelleden genoemde gegevens mag delen. In artikel 21, tweede lid, van de Wbni zijn organisaties genoemd waarmee het CSIRT voor digitale diensten de in dit artikellid genoemde gegevens mag delen. Met de in artikel 5 voorgestelde wijziging van de Wbni wordt de Minister van EZK hieraan toegevoegd, waardoor een rechtstreekse informatie-uitwisseling tussen het NCSC en het DTC, en tussen het CSIRT voor digitale diensten en het DTC mogelijk wordt gemaakt. In samenhang hiermee wordt in de voorgestelde artikelen 2, tweede lid, en 4 geregeld dat eenzelfde informatie-uitwisseling mogelijk is tussen het DTC enerzijds en het NCSC en het CSIRT voor digitale diensten anderzijds.

Met deze wettelijke bepalingen worden de onderscheidenlijke rollen en verantwoordelijkheden van de Minister van EZK en de Minister van JenV uitdrukkelijk in beide wetten benoemd. Daarnaast wordt hiermee voorzien in een wettelijke grondslag om elkaar ten behoeve van de onderscheidenlijke taken te voorzien van voor de uitoefening van die taken relevante informatie over digitale dreigingen, kwetsbaarheden en incidenten.

Naast de samenwerking binnen de overheid en met formele partners zoals benoemd in de Wbni, zal de Minister van EZK ook samenwerkingen aangaan met organisaties buiten de rijksoverheid. Denk hierbij aan maatschappelijke organisaties, onderzoeksinstituten, onderwijsinstellingen, cybersecurity bedrijven, decentrale overheden onafhankelijke cyber security onderzoekers.

Het onderwerp digitalisering van ondernemers is ook belegd bij de Minister van EZK. In het verlengde hiervan en in combinatie met de huidige taak van de Minister van EZK ondernemerschap te versterken, innovatievermogen te vergroten en randvoorwaarden voor economische groei te borgen is ervoor gekozen om de bredere taak en bevoegdheden van de Minister van EZK vast te leggen in een zelfstandige wet.

Bij de uitvoering van de taken zal rekening gehouden moeten worden met de Wet Markt en Overheid wat een onderdeel van de Mededingingswet is. Daarom is niet beoogd dat het DTC zal optreden als een ‘digitale brandweer’. Er zal buiten het bieden van handelingsperspectief geen directe ondersteuning worden verleend aan bedrijven bij het oplossen van digitale incidenten. Bedrijven zijn en blijven primair verantwoordelijk voor het treffen van passende maatregelen aangaande de beveiliging van hun informatiesystemen.

2.3 Motivering instrumentkeuze

Het verwerken en verspreiden van informatie (waaronder persoonsgegevens) door de overheid ten behoeve van de verbetering van de digitale weerbaarheid van niet-vitale bedrijven kan, conform het legaliteitsbeginsel, alleen als er een wettelijke taak aan ten grondslag ligt. Er is gekozen om de bevoegdheid van de Minister van EZK in deze vast te leggen in een formele wet. Hiermee wordt het bestaande stelsel van taken en bevoegdheden van de Rijksoverheid uitgebreid. Dit nieuwe wetsvoorstel staat naast de Wbni. Waar de Wbni, zoals eerder gezegd, zich richt op de rijksoverheid, vitale bedrijven en digitale dienstverleners zoals bedoeld volgens de Europese NIB- richtlijn, richt dit wetsvoorstel zich op het niet-vitale bedrijfsleven. In de Wbni zijn de taken van de Minister van JenV vastgelegd voor de rijksoverheid en vitale aanbieders en zijn de vakministers primair verantwoordelijk gemaakt voor het toezicht op de naleving van verplichtingen in de Wbni ten aanzien de digitale weerbaarheid van de onder hen vallende specifieke sectoren. Voor de Minister van EZK zijn deze taken naast de genoemde toezicht en naleving van de Wbni ook het voorzien van de CSIRT functie voor

digitaledienstverleners. De zorg voor het niet-vitale bedrijfsleven is niet in de Wbni belegd bij een vakminister en wordt met het onderhavige wetsvoorstel thans ondergebracht bij de Minister van EZK.

Naast bovengenoemde reden is er een tweede praktische reden om een specifieke wet op te stellen. De Wbni regelt namelijk primair de bevoegdheden van de Minister van Justitie en Veiligheid. Vanuit het stelseldenken is dit wetsvoorstel daarmee minder geschikt om daarin de bevoegdheden van de Minister van EZK in te verwerken. Door de bevoegdheden te scheiden is er duidelijkheid over de taken van beide ministers en kunnen beide zich richten op het verbeteren van de digitale veiligheid van de onder hun verantwoordelijkheid vallende doelgroep(en). In de praktijk zal hierbij uiteraard nauw worden samengewerkt door beide ministeries en uitvoerende organisatieonderdelen te weten het NCSC en het DTC.

2.4 Toepassing in Caribisch deel van het Koninkrijk

De taken en bevoegdheden van de Minister van EZK zoals omschreven in het onderhavige wetsvoorstel gelden voor Nederland inclusief de drie bijzondere gemeentes in het Caraïbisch gebied.

2.5 Monitoring en evaluatie

Het effect van het beleid wordt jaarlijks gemeten door het CBS als onderdeel van de meting 'ICT-gebruik bedrijven'[9]. Ook wordt er door het CBS-onderzoek gedaan naar de stand van cybersecurity in Nederland via de Cybersecuritymonitor.[10]

3. Verhouding tot andere nationale wetgeving

Dit wetsvoorstel regelt de informatiedeling door de rijksoverheid met het Nederlandse bedrijfsleven dat niet valt onder de werking van de Wbni. Daarmee richt het zich op bedrijven die vallen in de categorie niet-vitaal en geen digitaledienstverleners zijn. Deze groep bedrijven strekt zich uit van eenmansbedrijven (zzp) tot het grootbedrijf. Het wetsvoorstel heeft een directe relatie met de Wbni. Deze relatie zit in het feit dat het enerzijds de Minister van EZK de taak geeft de digitale weerbaarheid van niet- vitale bedrijven te verhogen en ten behoeve daarvan informatie te verwerken en te delen van twee partijen genoemd in de Wbni, zijnde de Minister van JenV (uitgevoerd door het NCSC) en de Minister van EZK (als CSIRT voor digitale diensten). Anderzijds zorgt dit wetsvoorstel ervoor dat voornoemde organisaties, NCSC en het CSIRT voor digitale diensten, vertrouwelijke en in bepaalde gevallen tot een aanbieder of dienstverlener herleidbare informatie (inclusief persoonsgegevens)

[9] https://www.cbs.nl/nl-nl/publicatie/2019/42/ict-kennis-en-economie-2019
[10] https://www.cbs.nl/nl-nl/publicatie/2019/37/cybersecuritymonitor-2019

mogen delen met de Minister van EZK. In dit wetsvoorstel is derhalve ook een wijziging van de Wbni opgenomen (artikel 5).

De benodigde maatregelen die bedrijven kunnen treffen ter bescherming van de gegevens, zoals geformuleerd in artikel 32 van de AVG, schrijven voor dat de verwerker en verwerkingsverantwoordelijke passende technische en organisatorische maatregelen dienen te treffen ter bescherming van persoonsgegevens. Als gevolg van dit wetsvoorstel zal de Minister van EZK het bedrijfsleven beter kunnen voorzien van praktische handvatten waarmee deels invulling kan worden gegeven door bedrijven aan de hiervoor genoemde technische en/of organisatorische maatregelen. Bedrijven zijn uiteraard zelf primair verantwoordelijk als het gaat om het treffen van maatregelen aangaande de beveiliging van hun systemen.

4. Gevolgen (m.u.v. financiële gevolgen)

Dit wetsvoorstel regelt de taak van de Minister van EZK om vertrouwelijke informatie, kwetsbaarheden en dreigingen (inclusief persoonsgegevens) te verwerken ten behoeve van het niet-vitale bedrijfsleven in Nederland. Er is geen regeldruk voorzien voor het Nederlandse bedrijfsleven. Er ontstaat geen verplichting voor bedrijven in Nederland om gebruik te maken van de informatie van het ministerie van EZK.

Met dit wetsvoorstel is er geen impact op de verhouding markt en overheid. De overheid beperkt zich tot het informeren en adviseren over kwetsbaarheden en dreigingen voor zover zij beschikt over die informatie. Het oplossen van incidenten en het nemen van preventieve maatregelen is aan bedrijven zelf, al dan niet met behulp van marktpartijen die dit voor hen kunnen organiseren.

4.1 Privacy

De persoonlijke levenssfeer in algemene zin wordt beschermd door artikel 10, eerste lid, van de Grondwet, artikel 8 van de Europese verklaring voor de rechten van de mens (EVRM), artikel 17 van het Internationaal verdrag inzake burgerlijke en politieke rechten (IVBPR) en artikel 7 van het Handvest van de gronden van de EU (Handvest). Bescherming van persoonsgegevens wordt daarnaast in het bijzonder beschermd door artikel 16, eerste lid, van het Verdrag betreffende de werking van de Europese Unie (VWEU), artikel 8 van het Handvest en artikel 10, tweede en derde lid, van de Grondwet. Ook in de Algemene verordening gegevensbescherming (AVG) staat de bescherming van persoonsgegevens centraal. De AVG werkt als verordening rechtstreeks in de Nederlandse rechtsorde.

Voor een goede uitvoering van de taken en bevoegdheden van de Minister van EZK, die met dit wetsvoorstel worden vastgelegd ter bevordering van de digitale weerbaarheid van bedrijven, zal het in voorkomend geval noodzakelijk zijn om persoonsgegevens te verwerken. Daarvan kan sprake zijn bij het doen van analyses om met name specifieke dreigingen te kunnen achterhalen en bij het contacteren van bedrijven om hen van informatie te kunnen voorzien. De bedrijfsgegevens die het hierbij betreft kunnen in sommige gevallen herleidbaar zijn tot een individu. Dat kan bijvoorbeeld het geval zijn bij een eenmansbedrijf of contactpersoon van een bedrijf. Hierbij gaat het om 'gewone' persoonsgegevens waarbij niet meer gegevens worden verwerkt dan strikt noodzakelijk, en deze niet voor andere doeleinden worden gebruikt dan waarvoor zij oorspronkelijk zijn verzameld.

PM: advies Autoriteit persoonsgegevens.

5. Uitvoering

Ter uitvoering van de in dit wetsvoorstel genoemde taken is de inrichting van een informatiedienst voorzien. Deze dienst wordt ingericht volgens de binnen de rijksoverheid geldende richtlijnen en kaders zoals de Baseline Informatiebeveiliging Overheid (BIO). Deze informatiedienst zal ingericht worden om informatie van binnen en buiten de overheid te ontvangen, beoordelen, verwerken en verspreiden voor zover relevant voor de doelgroep van dit wetsvoorstel. De informatiedienst zal hierbij zoveel mogelijk gebruik gaan maken van digitale systemen en processen.

6. Toezicht en handhaving

Er is geen direct toezicht en handhaving op basis van dit wetsvoorstel voorzien. Ondernemen is risico's afwegen en risico's nemen, bedrijven zijn dan ook, behoudens wettelijke kaders, autonoom om beslissingen te nemen over hun bedrijfsvoering.

7. Financiële gevolgen

De financiële gevolgen van dit wetsvoorstel zijn een toevoeging op de begroting van het ministerie van EZK met in eerste instantie 2 miljoen euro ten behoeve van de inrichting en de start van de informatiedienst ter uitvoering van deze taak.

Voor de in dit wetsvoorstel beschreven taken en bevoegdheden van de Minister van EZK, uitgevoerd door het DTC, is op de begroting van het ministerie van EZK structureel € 2,5 miljoen beschikbaar. Hiermee is er financiële dekking voor zowel de personeelsuitgaven als de materiële uitgaven voor wat betreft het verstrekken van dreigingsinformatie aan de doelgroep en het stimuleren van de

ontwikkeling van de samenwerkingsverbanden. Voor genoemde taken is een minimale capaciteit voorzien van 9 fte resp. 3 fte en een materieel budget van € 400.000 voor ICT en communicatie.

8. Advies en consultatie

PM: in te vullen na advies en (internet)consultatie.

B. Artikelsgewijze toelichting

Artikel 1 (Begripsbepalingen)

Het begrip “bedrijf” slaat zowel op natuurlijke personen als op privaatrechtelijke rechtspersonen die in Nederland gevestigd zijn, bedrijfsmatige activiteiten uitvoeren en die niet onder de werkingssfeer van de Wet beveiliging netwerk- en informatiesystemen (Wbni) vallen. Vitale aanbieders en digitaledienstverleners behoren derhalve niet tot de doelgroep van dit wetsvoorstel.

De begrippen incident en netwerk- en informatiesysteem hebben dezelfde betekenis als in de NIB-richtlijn en in de Wbni. Dit om eenheid in terminologie te waarborgen.

Incident: elke gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen.

Netwerk- en informatiesysteem:

a) een elektronisch communicatienetwerk in de zin van artikel 2, onder a), van Richtlijn 2002/21/EG;

b) een apparaat of groep van geïnterconnecteerde of bij elkaar behorende apparaten, waarvan een of meer, overeenkomstig een programma, digitale gegevens automatisch verwerkt of verwerken, of

c) digitale gegevens die via in de punten a) en b) bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan.

Het begrip CSIRT voor digitale diensten heeft dezelfde betekenis als in de Wbni. Dit om eenheid in terminologie te waarborgen.

Artikel 2 (Taken van Onze Minister)

Het artikel bevat een opsomming van de taken van de Minister van EZK op het terrein van digitale weerbaarheid van bedrijven, ten behoeve waarvan verwerking van gegevens, waaronder

persoonsgegevens, aangewezen is, en omschrijft de doeleinden van die taken. Zie voor een nadere toelichting hierop paragraaf 2.2 van het algemeen deel van deze memorie.

Artikel 3 (Verstrekking gegevens aan Onze Minister)

Het eerste lid voorziet in een wettelijke bevoegdheid voor de Minister van EZK om rechtspersonen (overheden of private partijen) of organen daarvan om gegevens te vragen die noodzakelijk zijn voor de uitoefening van de in artikel 2 genoemde taken. Het gaat hierbij niet om een bevoegdheid tot het vorderen van gegevens; de rechtspersoon of het orgaan daarvan waaraan het verzoek is gericht is niet verplicht tot medewerking.

Ingevolge het doelbindingsbeginsel van artikel 5, eerste lid, onder b, AVG moeten persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen zij vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt. De AVG biedt echter de mogelijkheid om onder voorwaarden door middel van nationale bepalingen de verdere verwerking van persoonsgegevens mogelijk te maken, ook als dat geschiedt voor een doel dat niet verenigbaar is met het doel waarvoor de persoonsgegevens zijn verkregen. Het tweede lid van artikel 3 geeft toepassing aan die bevoegdheid. Dat is een noodzakelijke en evenredige maatregel ter waarborging van meerdere in artikel 23, eerste lid, AVG, genoemde belangen, waaronder onder meer de openbare veiligheid.

Artikel 4 (Verstrekking van vertrouwelijke gegevens door Onze Minister)

Artikel 4, eerste lid, regelt de verstrekking door de Minister van EZK, ter uitvoering van de in artikel 2, eerste en tweede lid, onder c en d, bedoelde taken, aan derden, waaronder de Minister van JenV en het CSIRT voor digitale diensten, van vertrouwelijke gegevens met betrekking tot bedrijven, zoals gegevens over de identiteit van een bij een incident betrokken bedrijf of specifieke gegevens over de beveiliging van een elektronisch informatiesysteem van een bedrijf. Artikel 4, eerste lid, staat uiteraard niet in de weg aan verstrekking door het DTC aan derden van gegevens die niet vertrouwelijk zijn.

Het eerste lid regelt dat bij de Minister van EZK berustende vertrouwelijke gegevens slechts ter uitvoering van de in artikel 2 genoemde taken aan derden worden verstrekt, indien aldaar de geheimhouding van de gegevens voldoende is gewaarborgd en voldoende is gewaarborgd dat de gegevens uitsluitend worden gebruikt voor het doel waarvoor zij worden verstrekt. Het eerste lid ziet op vertrouwelijke gegevens met betrekking tot bedrijven, dus niet op andere vertrouwelijke gegevens, zoals persoonsgegevens die niet herleidbaar zijn tot een bedrijf. Voor de verwerking van persoonsgegevens door de Minister van EZK geldt de AVG.

Ter uitvoering van de in artikel 2, tweede lid, onder c, bedoelde taak regelt artikel 4, tweede lid, de verstrekking door de Minister van EZK aan de Minister van JenV van vertrouwelijke gegevens met betrekking tot vitale aanbieders en andere aanbieders die onderdeel zijn van de rijksoverheid.

Ter uitvoering van de in artikel 2, tweede lid, onder d, bedoelde taak regelt artikel 4, derde lid, de verstrekking door de Minister van EZK aan het CSIRT voor digitale diensten van vertrouwelijke gegevens met betrekking tot digitaledienstverleners.

Deze bevoegdheid maakt het mogelijk om vertrouwelijke gegevens over andere partijen dan eigen doelgroep (bedrijven) met de relevante overheidsorganisaties te delen.

Bij het begrip vertrouwelijke gegevens kan worden gedacht aan informatie over netwerk- en informatiesystemen die een bedrijf gebruikt bij zijn dienstverlening. Ook vertrouwelijke gegevens die herleid kunnen worden tot een bedrijf, vitale aanbieder of een digitaledienstverlener vallen hieronder.

Het is voor de toepassing van artikel 4 niet relevant of de Minister van EZK de gegevens heeft verkregen van de partij zelf of anderszins, zoals door analyse van de Minister van EZK of ontvangst van een andere organisatie.

Artikel 5 (wijziging Wet beveiliging netwerk- en informatiesystemen)

In de artikelen 3, tweede lid, en 20, tweede lid, van de Wbni worden partijen genoemd waarmee het NCSC in voorkomende gevallen gegevens in een beperkte kring van derden mag delen. Hierbij kan het ook gaan om persoonsgegevens en vertrouwelijke gegevens die herleid kunnen worden tot een aanbieder.

In artikel 21, tweede lid, van de Wbni worden partijen genoemd waarmee het CSIRT voor digitale diensten in voorkomende gevallen vertrouwelijke gegevens die herleid kunnen worden tot een digitaledienstverlener, zonder diens instemming, in een beperkte kring van derden mag delen.

Ten behoeve van de taakuitoefening door de Minister van EZK op grond van dit wetsvoorstel wordt met de voorgestelde wijziging van de Wbni de Minister van EZK toegevoegd aan de kring van derden waarmee het NCSC en het CSIRT voor digitale diensten in voorkomende gevallen persoonsgegevens en vertrouwelijke herleidbare gegevens mogen delen.