Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2023–2024

36 270 Regels ter bevordering van de digitale weerbaarheid van bedrijven (Wet bevordering digitale weerbaarheid bedrijven)

E

NOTA NAAR AANLEIDING VAN HET TWEEDE VERSLAG

Ontvangen 19 juni 2024

Het wetsvoorstel en de nota naar aanleiding van het verslag hebben de commissie aanleiding gegeven tot het maken van de volgende opmerkingen en het stellen van de volgende vragen.

Inleiding

In 2017 is het Digital Trust Center (DTC) opgericht als onderdeel van het Ministerie van Economische Zaken en Klimaat (EZK). Het DTC heeft als missie bedrijven weerbaarder te maken tegen cyberdreigingen. De behoefte bestaat om het bedrijfsleven niet alleen over algemene, maar ook over specifieke digitale dreigingen en kwetsbaarheden te informeren. Deze uitbreiding van de informatievoorziening vraagt een verdere inbedding van de taken en bevoegdheden van de Minister van EZK. Het wetsvoorstel biedt de expliciete wettelijke grondslag om in het kader van de taakuitvoering persoonsgegevens te verwerken.
Naar aanleiding van dit voorstel hebben de fractieleden van de ***BBB*** *enkele vragen aan de regering.*

Met belangstelling heb ik kennisgenomen van de vragen en opmerkingen die door de leden van de fractie van BBB zijn gesteld in het tweede verslag van de vaste commissie voor Economische Zaken en Klimaat van 11 juni 2024. In deze nota naar aanleiding van het tweede verslag ga ik graag in op de vragen en opmerkingen, waarbij ik de volgorde van het verslag volg. De tekst van het verslag is schuingedrukt, de beantwoording niet.

Vragen en opmerkingen van de leden van de BBB-fractie

Het delen van gevoelige dreigingsinformatie met bedrijven die hun informatiebeveiliging onvoldoende op orde hebben kan datalekken van bedrijfsgevoelige/privacygevoelige informatie juist in de hand werken. De

kst-36270-E
ISSN 0921 - 7371
's-Gravenhage 2024

regering zegt informatie te delen mits de beveiliging op orde is.[1] Hoe wordt dit bepaald?

Anders dan de leden van de BBB-fractie veronderstellen, is het bij het informeren van niet-vitale bedrijven over cyberdreigingen, kwetsbaarheden of incidenten geen factor of de cybersecurity van een organisatie verder op orde is. Door bij de overheid bekende informatie over een ernstige cyberdreiging, kwetsbaarheid of incident te verstrekken aan het niet-vitale bedrijfsleven stelt het Digital Trust Center deze bedrijven in staat om op basis van de informatie en een algemeen handelingsperspectief zelf te beoordelen of, en zo ja, in welke mate, zij maatregelen moeten treffen ter mitigatie van een kwetsbaarheid. De gedeelde informatie dient ertoe om een digitale dreiging af te weren of om een daadwerkelijke inbreuk op te lossen. Deze dienstverlening is vergelijkbaar met een attentie vanuit de politie dat de achterdeur van een woning niet goed op slot is gedraaid. Bij het informeren van niet-vitale bedrijven over cyberdreigingen, kwetsbaarheden of incidenten wordt informatie gedeeld die uitsluitend voor deze organisaties relevant is.
Voor wat betreft het delen van informatie met individuele bedrijven betracht de Minister van Economische Zaken en Klimaat (EZK) uiteraard grote zorg. Het is belangrijk om dreigingsinformatie zo snel mogelijk met desbetreffende organisaties te delen omdat zij vaak niet op de hoogte zijn van het feit dat zij mogelijk kwetsbaar zijn. In veel voorkomende gevallen zijn kwaadwillenden hiervan juist wél op de hoogte, en gaan zij online op zoek (scannend) naar deze kwetsbare systemen/organisaties.

De regering hanteert voor de medewerkers die deze wet uitvoeren een Data Protection Impact Assessment (DPIA). De Minister van EZK bepaalt wie welke toegang krijgt, er is een screening en men krijgt toegang op basis van «need to know». De fractie van de BBB kan zich voorstellen dat deze informatie interessant is voor cybercriminelen. Wordt ook gekeken in hoeverre deze medewerkers chantabel zijn? Hoe is de beveiliging van deze medewerkers geregeld? In hoeverre is er voldoende personeel beschikbaar?

Het Digital Trust Center (DTC) heeft een Data Protection Impact Assessment (DPIA) uitgevoerd met betrekking tot voorliggend wetsvoorstel. Hierin staan de genomen maatregelen om de verwerkte persoonsgegevens te beschermen. Een van de maatregelen is dat het personeel dat werkt met deze gegevens in het bezit dient te zijn van een verklaring van geen bezwaar (vgb), verkregen na de uitvoering van een veiligheidsonderzoek door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). In een veiligheidsonderzoek wordt een oordeel gevormd over de kwetsbaarheid van betrokkene bij het vervullen van een vertrouwensfunctie en wordt onder andere gekeken naar de gevoeligheid van de betrokkene voor chantage.
Om de beveiliging van de medewerkers van het DTC en de gevoelige gegevens waarmee wordt gewerkt, te waarborgen, worden werkzaamheden uitgevoerd in een aparte ruimte die alleen toegankelijk is met extra autorisatie.
In tijden van krapte op de arbeidsmarkt is het vinden van gekwalificeerd personeel een breed gedeeld probleem, dit is ook merkbaar in de cybersecuritywereld. Tot op heden is het DTC zelf echter nog niet tegen belemmerende problemen aangelopen wat betreft het aantrekken van personeel.

[1] Reactie VNO NCW en MKB Nederland op internetconsultatie voorstel Wet bevordering digitale weerbaarheid bedrijfsleven.

Wat is de stand van zaken van de samenwerkingsafspraken tussen het Nationaal Cyber Security Centrum (NCSC) en het DTC?

De samenwerking tussen het DTC en het NCSC werd in eerste instantie ondersteund door samenwerkingsafspraken. Dit waren tevens de eerste stappen richting het integratietraject van de drie overheidsorganisaties die zich bezighouden met cybersecurity: het DTC, het NCSC en het Computer Security Incident Response Team (CSIRT) voor digitale diensten. Inmiddels wordt er, zoveel als mogelijk, intensief samengewerkt tussen het DTC en het NCSC. Dit gebeurt op diverse terreinen, er wordt bijvoorbeeld gezamenlijk gewerkt aan de ontwikkeling van het cyberweerbaarheidsnetwerk.[2] Deze inspanningen dragen bij aan de realisatie dat beide organisaties conform planning per 1 januari 2026 volledig als één geïntegreerde entiteit zullen opereren.

In hoeverre overweegt de regering een toekomstig samengaan in het kader van efficiency en de schaarste aan vakkundig personeel?

Zoals aangegeven in paragraaf 2.4 van de memorie van toelichting bij het voorliggend wetsvoorstel en in de brief aan de Tweede Kamer van 7 september 2022 worden de krachten van het NCSC, het DTC en het CSIRT voor digitale diensten (CSIRT-DSP) gebundeld.[3] Het bundelen van kennis en informatie rondom cybersecurity en dienstverlening bij grote incidenten vergroot de digitale weerbaarheid van Nederland. Deze vernieuwde organisatie gaat alle organisaties in Nederland – groot of klein, publiek of privaat, vitaal en niet-vitaal – van passende informatie en kennis voorzien. Door het creëren van één uitvoeringsorganisatie kan de Rijksoverheid haar cybersecuritycapaciteit efficiënter en effectiever inzetten. De bundeling van krachten zorgt ook voor een efficiëntieslag op het gebied van gezamenlijke bedrijfsvoering, huisvesting en ICT.
De eerstvolgende mijlpaal van de integratie is het afronden van de initiële fase in oktober 2024, welke gevolgd zal worden door de optimalisatiefase die loopt tot 1 januari 2026. Op die datum dient de vernieuwde organisatie de verschillende taken in samenhang en in voldoende mate uit te voeren.

In hoeverre is de beoogde capaciteit en het budget van het DTC toereikend, ook gezien de toename van cyberdreiging en de mogelijke overlap tussen vitale en niet-vitale bedrijven?

Het DTC bedient uitsluitend het niet-vitale bedrijfsleven en zal in de uitvoering van de taken zoveel als mogelijk efficiëntie en effectiviteit nastreven en gebruik maken van digitale processen. Er wordt ingezet op een geleidelijke doorgroei van het DTC waarin periodiek zal worden geëvalueerd of de inzet van mensen en budgetten gelijklopen met de ambities van het kabinet en de vraag vanuit het bedrijfsleven.
Op de EZK-begroting is met versterking uit het vorige coalitieakkoord € 8,1 miljoen per jaar beschikbaar in de periode 2024–2026 en vanaf 2027 structureel € 9,0 miljoen per jaar. Hiermee is het totaal structureel beschikbare bedrag voor het DTC momenteel voldoende voor de uitvoering van dit wetsvoorstel en is er in de basis financiële dekking voor zowel de personeelsuitgaven als de materiële uitgaven voor wat betreft het verstrekken van algemene en specifieke dreigingsinformatie aan de doelgroep en het stimuleren van samenwerking en samenwerkingsverbanden.

Waarom kan de rechtspersoon op grond van artikel 3, tweede lid persoonsgegevens ook aan de Minister van EZK verstrekken als de

[2] Kamerstuk 26 643, nr. 1176.
[3] Kamerstuk 26 643, nr. 927.

verstrekking onverenigbaar is met de doeleinden waarvoor de persoonsgegevens zijn verzameld? Welk doel dient dit? Waarom is hier gekozen voor een kan-bepaling? Is het aanleveren van gegevens door niet-vitale bedrijven vrijblijvend en vrijwillig? De leden van de BBB-fractie verzoeken u om een toelichting.

Voorgesteld artikel 3, eerste lid, van het wetsvoorstel voorziet in een wettelijke bevoegdheid voor de Minister van EZK om rechtspersonen of organen daarvan om gegevens te vragen die noodzakelijk zijn voor de uitoefening van de in artikel 2, eerste lid, van het wetsvoorstel genoemde taken. Er is gekozen voor een kan-bepaling omdat het hierbij niet gaat om een bevoegdheid tot het vorderen van gegevens; de rechtspersoon of het orgaan daarvan waaraan het verzoek is gericht is niet verplicht tot medewerking. Het aanleveren van gegevens door niet-vitale bedrijven is vrijblijvend en vrijwillig.
Het kan voorkomen dat een rechtspersoon de gevraagde gegevens aan de Minister van EZK wil verstrekken maar dat de verstrekking ervan in strijd zou zijn met het doel waarvoor de persoonsgegevens zijn verzameld. Ingevolge het doelbindingsbeginsel van artikel 5, eerste lid, onder b, Algemene verordening gegevensbescherming (AVG) moeten persoonsgegevens immers 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.

Waarom kan de Minister van EZK de vertrouwelijke gegevens met betrekking tot een vitale aanbieder zonder diens toestemming verstrekken aan de Minister van J&V/Computer Incident Response Team (CSIRT) ten behoeve van diens taken als bedoeld in artikel 3, eerste titel van de Wet beveiliging netwerk- en informatiesystemen? Waarom is ervoor gekozen geen toestemming te vragen? In hoeverre en op welke wijze wordt de vitale aanbieder hierover geïnformeerd?

Bij de uitvoering van diens taken kan de Minister van EZK beschikken over vertrouwelijke gegevens die niet relevant zijn voor de eigen doelgroep (niet-vitale bedrijven), maar wel voor de doelgroep van, bijvoorbeeld, het NCSC (vitale aanbieders en rijksoverheidsorganisaties). Om de digitale weerbaarheid van de Nederlandse samenleving als geheel te versterken of om nadelige maatschappelijke gevolgen te voorkomen, is het gewenst dat deze gegevens met de voor de desbetreffende doelgroep verantwoordelijke overheidsorganisatie kunnen worden gedeeld. Hierom bevat het wetsvoorstel een grondslag op basis waarvan de Minister van EZK vertrouwelijke gegevens met betrekking tot vitale aanbieders en rijksoverheidsorganisaties met de Minister van JenV kan delen, ten behoeve van de uitvoering van de taken die het NCSC namens die Minister uitvoert. Het wetsvoorstel bevat overigens ook een vergelijkbare bepaling ten aanzien van verstrekking van informatie door het DTC aan het CSIRT voor digitale diensten.
Ten aanzien van het delen van vertrouwelijke gegevens is in dit wetsvoorstel aansluiting gezocht bij de systematiek die geldt op basis van de Wet beveiliging netwerk- en informatiesystemen voor het verstrekken van vertrouwelijke tot aanbieders herleidbare gegevens door het NCSC aan andere organisaties.

Hoe gaat de Minister van EZK op basis van deze wet de weerbaarheid van niet-vitale bedrijven versterken tegen digitale dreiging? In hoeverre wordt de advisering van het DTC voorzien van een handelingsperspectief?

Het DTC beschikt over informatie over kwetsbare of gehackte systemen bij Nederlandse niet-vitale bedrijven. Dit kan bijvoorbeeld gaan over software waar een fout in zit, systemen waarop malware is geïnstalleerd door cybercriminelen of systemen die elk moment misbruikt kunnen worden voor een ransomware aanval. Om betrokkenen te informeren verzendt het DTC een waarschuwingsbericht per e-mail. In deze e-mail wordt naast informatie over een specifieke dreiging door het DTC ook een zo praktisch mogelijk handelingsperspectief aangereikt zodat het bedrijf ook weet welke vervolgstap(pen) het kan nemen.

Hoe worden toezicht- en handhaving geregeld?

Zoals aangegeven in paragraaf 8.6 van de memorie van toelichting bij dit wetsvoorstel is er geen sprake van toezicht en handhaving. Ook geldt op grond van het onderhavige voorstel geen verplichtingen voor de doelgroep van dit wetsvoorstel, te weten de niet-vitale bedrijven.

Wat zijn de mogelijke gevolgen van deze wet voor de regeldruk van bedrijven?

Er is geen regeldruk voorzien voor het Nederlandse bedrijfsleven. Er ontstaat geen verplichting voor bedrijven in Nederland om gebruik te maken van de informatie vanuit het Ministerie van EZK.
Op basis van het voorliggend wetsvoorstel heeft de Minister van EZK de mogelijkheid om bedrijven te vragen om informatie te delen. Het delen van informatie op basis van een dergelijk verzoek is volledig vrijwillig. Mocht een bedrijf hier aan mee willen werken dan wordt de regeldruk die hiermee in potentie ontstaat verwaarloosbaar geacht, aangezien er voor een dergelijk verzoek geen vormvereiste geldt en omdat dit om een incidentele en vrijwillige activiteit gaat.
Het Adviescollege Toetsing Regeldruk (ATR) heeft geen aanleiding gezien om een formeel advies uit te brengen en heeft het voorstel ambtelijk afgedaan.[4]

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens

[4] Kamerstuk 36 270, nr. 3.