AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

De Minister van Veiligheid en Justitie

Postbus 20301
2500 EH DEN HAAG

Datum	Ons kenmerk	Uw brief van
25 oktober 2017	z2017-4917	16 juni 2017

Onderwerp
Adviesverzoek concept-Cybersecuritywet

Geachte ,

Bij brief van 16 juni 2017 heeft u de Autoriteit Persoonsgegevens (AP) gevraagd op grond van het bepaalde in artikel 51, tweede lid, van de Wet bescherming persoonsgegevens (Wbp) te adviseren over het concept-wetsvoorstel implementatie EU-richtlijn netwerk- en informatiebeveiliging (concept-Cybersecuritywet; hierna: het wetsvoorstel).

Met betrekking tot het onderhavige wetsvoorstel is een internetconsultatie opengesteld van 16 juni 2017 tot en met 16 juli 2017. Naar aanleiding van deze internetconsultatie zijn wijzigingen in het wetsvoorstel aangebracht. De herziene versie van het concept-wetsvoorstel heeft de AP op 23 augustus 2017 ontvangen.

De AP voldoet hiermee aan uw verzoek.

Datum
25 oktober 2017

Ons kenmerk
z2017-4917

Inhoud van het wetsvoorstel
Dit wetsvoorstel implementeert de EU-richtlijn netwerk- en informatiebeveiliging[1] (verder te noemen: NIB Richtlijn).

De NIB Richtlijn

De NIB richtlijn:

- schrijft voor dat lidstaten een nationale strategie voor netwerk- en informatiebeveiliging ontwikkelen;
- creëert een Europees/nationaal netwerk van organen die een rol spelen bij netwerk- en informatiebeveiliging. Dit zijn op lidstatelijk niveau de " bevoegde autoriteit"(artikel 8 lid 1 en 2), het "centrale contactpunt" (artikel 8 lid 3) en het CSIRT (Computer Security Incident Response Team; artikel 9), en op Europees niveau de "Cooperation group" (artikel 11);
- stelt (globale) beveiligingseisen aan aanbieders van essentiële diensten[2] en digitale dienstverlening[3];
- creëert een meldplicht voor ICT-incidenten bij aanbieders van essentiële diensten en digitale dienstverlening.

Het wetsvoorstel

Het wetsvoorstel benoemt het "centrale contactpunt" (artikel 2 sub a), meerdere CSIRTs (artikel 2 sub b en artikel 4 lid 2 sub b) en meerdere "bevoegde autoriteiten" (artikel 4 lid 1 en artikel 4 lid 2 sub a).

In artikel 5 wordt de aanwijzing van zogenaamde vitale aanbieders[4] gedelegeerd naar een AMvB. De aanwijzing kan ook worden gedaan door een bij deze AMvB aangewezen bestuursorgaan.

De artikelen 7-8 bevatten de (globale) beveiligingseisen aan aanbieders van essentiële diensten en digitale dienstverlening (met de mogelijkheid tot nadere detaillering bij of krachtens AMvB (artikel 9)).

[1] Richtlijn (EU) 2016/1148.
[2] Essentiële diensten zijn diensten zonder welke de maatschappij niet meer kan functioneren. Denk aan energie, drinkwater en het betalingsverkeer. De NIB Richtlijn draagt de lidstaten op uiterlijk 9 november 2018 voor hun gebied de essentiële diensten aan te wijzen.
[3] Met digitale dienstverlening wordt, in het kader van deze Richtlijn, gedoeld op onlinemarktplaatsen, onlinezoekmachines en cloudcomputerdiensten.
[4] Dit begrip is ruimer dan "essentiële diensten" in de Richtlijn. Het omvat namelijk ook aanbieders van andere diensten waarvan de continuïteit van "vitaal belang" is (zie de definitie in artikel 1 wetsvoorstel).
Overigens hebben "essentieel" en "vitaal" in dit verband ongeveer dezelfde betekenis, waardoor dit onderscheid – althans voor de AP – niet helder is. Wetgevingstechnisch is het onderscheid wel verklaarbaar: aanbieders van beide soorten diensten vallen onder de definitie van "vitale aanbieder" in het wetsvoorstel, maar alleen voor wat betreft "essentiële diensten" is sprake van implementatie van richtlijn (EU) 2016/1148, waardoor sommige bepalingen in het wetsvoorstel ter omzetting van de richtlijn alleen zien op aanbieders van essentiële diensten en niet op alle vitale aanbieders. Maar het naast elkaar gebruiken van beide termen leidt mogelijk tot spraakverwarring en/of afbakeningsproblemen. Dit behoeft mogelijk enige aandacht.

De artikelen 10-15 beschrijven de meldplicht voor ICT-incidenten.

De verwerking van gegevens – waaronder persoonsgegevens – is geregeld in de artikelen 16-20.

De artikelen 21-26 betreffen de handhaving van de bij deze wet gestelde voorschriften.

Advies
Het wetsvoorstel geeft de AP aanleiding tot het maken van de volgende op- en aanmerkingen.

Vooraf
Zoals ook vermeld in de Memorie van Toelichting van het conceptwetsvoorstel is vanaf 25 mei 2018 de Algemene verordening gegevensbescherming (AVG) van toepassing. Uw voorstel is door de AP aan de AVG getoetst en niet meer aan de huidige Wbp, omdat de Cybersecuritywet naar verwachting niet vóór mei 2018 in werking zal treden. In dat kader acht de AP het echter wel van belang het volgende op te merken. De AVG beoogt in de gehele Europese Unie een uniforme toepassing van de regels inzake bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen in verband met de verwerking van persoonsgegevens te bewerkstelligen. Hiertoe is het onder meer noodzakelijk dat de toezichthoudende autoriteiten in de lidstaten van de EU gezamenlijk bijdragen aan de ontwikkeling van een uniforme uitleg van bepalingen van de AVG. Gelet op de omstandigheid dat de AVG pas vanaf 25 mei 2018 van toepassing is, kunnen inzichten met betrekking tot de toepassing van de AVG – door bijvoorbeeld benodigde afstemming met andere toezichthouders – in de toekomst invloed hebben op het oordeel van de AP.

Wetsvoorstellen dienen te voldoen aan artikel 8 van het Handvest van de grondrechten van de Europese Unie (Handvest), artikel 16 van Verdrag betreffende de werking van de Europese Unie (VWEU), artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en artikel 10 van de Grondwet.
Artikel 8 van het Handvest bepaalt onder meer dat persoonsgegevens eerlijk en voor bepaalde doeleinden moeten worden verwerkt, en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Artikel 16 VWEU bepaalt dat eenieder in de Europese Unie recht heeft op bescherming van zijn persoonsgegevens. Op grond van artikel 8 EVRM is geen inmenging van enig openbaar gezag toegestaan in de uitoefening van het recht op respect voor zijn privéleven, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. Artikel 10, eerste lid, van de Grondwet bepaalt dat een ieder recht heeft op eerbiediging van zijn persoonlijke levenssfeer, behoudens bij of krachtens de wet te stellen beperkingen.
Bij de toepassing van de in voornoemde grondrechtbepalingen opgenomen beperkingsclausules spelen het proportionaliteits- en het subsidiariteitsbeginsel een belangrijke rol. Deze beginselen volgen uit het woord 'noodzakelijk' zoals opgenomen in elk van de bovengenoemde grondslagen. Het

proportionaliteitsbeginsel houdt in dat de inbreuken op de belangen van de bij de verwerking van persoonsgegevens betrokkene niet onevenredig mogen zijn in verhouding tot het met de verwerking te dienen doel. Ingevolge het subsidiariteitsbeginsel dient het doel waarvoor de persoonsgegevens worden verwerkt niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige, wijze te kunnen worden verwerkelijkt.

I. Het belang van de NIB Richtlijn

De NIB Richtlijn beschrijft in overwegingen (1) en (2) het motief van de richtlijn:

(1) Netwerk- en informatiesystemen en -diensten spelen een cruciale rol in de samenleving. De betrouwbaarheid en beveiliging ervan zijn essentieel voor economische en maatschappelijke activiteiten, en met name voor de goede werking van de interne markt.

(2) De omvang, de frequentie en de gevolgen van beveiligingsincidenten nemen toe en vormen een grote bedreiging voor de goede werking van netwerk- en informatiesystemen. Die systemen kunnen ook een doelwit worden van opzettelijke schadelijke acties die bedoeld zijn om de werking van de systemen te verstoren of te onderbreken. Zulke incidenten kunnen de economische bedrijvigheid belemmeren, aanzienlijke financiële verliezen opleveren, het gebruikersvertrouwen ondermijnen en de economie van de Unie ernstige schade toebrengen.

De AP onderschrijft het nog steeds toenemende belang van veilige digitale systemen.

II. Raakvlakken NIB Richtlijn – privacybescherming

De NIB Richtlijn constateert terecht dat bij veel incidenten persoonsgegevens in het geding zijn.[5] Als het niveau van de informatiebeveiliging wordt verhoogd zoals de NIB Richtlijn beoogt, dan heeft dat (ook) een positieve impact op de bescherming van persoonsgegevens.

Het onderwerp informatiebeveiliging is een wezenlijk onderdeel van de bescherming van persoonsgegevens en dat zal straks onder de Algemene Verordening Gegevensbescherming (AVG) niet anders zijn. De AP en haar Europese collega's hebben door voorlichting en actief toezicht een belangrijke bijdrage geleverd aan de ontwikkeling van het "leerstuk" informatiebeveiliging. Beveiliging van persoonsgegevens is immers geen op zich zelf staande discipline maar volgt dezelfde heuristieken als informatiebeveiliging in andere domeinen[6].

[5] Overweging (63).
[6] Zoals bijvoorbeeld de procesindustrie.

III. Nationale strategie (NL)

De NIB Richtlijn verplicht de lidstaten tot het formuleren van een nationale cybersecurity strategie.[7] De MvT stelt – onder verwijzing naar Aanwijzing voor de regelgeving 332 – terecht dat deze verplichting niet in wetgeving behoeft te worden geïmplementeerd.[8]

De MvT verwijst naar de Nationale Cybersecurity Strategie 2013. De AP merkt op dat het hierin opgenomen Actieplan liep van 2014 tot 2016 en dus niet meer actueel is.

IV. Informatie-uitwisseling en coördinatie

Goede informatie-uitwisseling is cruciaal voor effectief *incident management* en *emergency response*. Informatie-uitwisseling bij ernstige beveiligingsincidenten is voor Nederland een belangrijk aandachtspunt.[9]

In dat kader vallen vier zaken in het wetsvoorstel op:

1. Voor ernstige ICT-incidenten is gekozen voor een dubbele meldplicht (bij CSIRT en bij de bevoegde autoriteit) .[10] Deze implementatiekeuze vloeit niet rechtstreeks voort uit de NIB Richtlijn.[11]

2. Ingevolge artikel 33 AVG worden datalekken gemeld bij de AP. Deze melding zal naar verwachting volledig los komen te staan van de meldplichten in het wetsvoorstel. De AP melding zal – voor zover bekend - evenmin worden geïntegreerd in het in de MvT aangekondigde elektronisch formulier waarin de melder met één handeling aan beide Cybersecuritywet-meldplichten kan voldoen.[12] Dit is niet alleen lastig voor de melder, het maakt ook dat een met de AP gecoördineerde response of een gezamenlijke analyse bij een inbreuk op de beveiliging van persoonsgegevens[13] in de praktijk minder goed mogelijk zal zijn.
   De AP adviseert u daarom – in overleg met de AP – de wenselijkheid en haalbaarheid te onderzoeken van gecoördineerde incidentopvolging en informatie-uitwisseling, opdat aan deze bezwaren tegemoet kan worden gekomen.

[7] artikel 7 NIB Richtlijn.
[8] MvT p. 4.
[9] Cyber Security Raad advies "Naar een landelijk dekkend stelsel van informatieknooppunten" (2017), p. 3.
[10] MvT p. 3.
[11] Zie artikel 14 lid 3 en 16 lid 3 NIB Richtlijn.
[12] MvT p. 31.
[13] Voor zover het een vitale dienst of digitale dienstverlener betreft.

3. Overweging (63) van de NIB Richtlijn luidt als volgt:

   In veel gevallen worden persoonsgegevens aangetast als gevolg van incidenten. Daarom moeten de bevoegde autoriteiten en de autoriteiten voor gegevensbescherming samenwerken en informatie over alle relevante zaken uitwisselen om inbreuken in verband met persoonsgegevens als gevolg van incidenten aan te pakken.

   Deze overweging pleit ervoor om samenwerking en informatie-uitwisseling tussen de AP en de autoriteiten in de Cybersecuritywet te regelen, maar een regeling hiervoor ontbreekt.

4. Het wetsvoorstel richt zich uitsluitend op zogenaamde vitale aanbieders en digitale dienstverleners[14]. Echter ook bij andere partijen kunnen zich identieke beveiligingsincidenten voordoen – zij het dan met minder impact. Weliswaar biedt artikel 15 van het wetsvoorstel de mogelijkheid van een vrijwillige melding bij een nader aan te wijzen "instantie", maar dat is – afhankelijk van de follow-up van zo'n vrijwillige melding èn de positionering van deze "instantie"- wellicht niet genoeg voor een landelijk dekkende, gecoördineerde, *emergency response*. Bovendien missen deze andere partijen mogelijk straks informatie om ernstige ICT-problemen op te lossen terwijl deze informatie wel (elders) beschikbaar is.[15] De AP verwijst in dit verband naar het advies van de Cyber Security Raad om een Digital Trust Centre en een Nationaal Detectie Netwerk op te richten.[16]

V. De overheid als vitale aanbieder

De NIB Richtlijn betreft – naast "digitale dienstverleners"[17] - de sectoren als bedoeld in Bijlage II van de Richtlijn. Het wetsvoorstel biedt de mogelijkheid ook daarbuiten *incident management* en *emergency response* te reguleren (artikel 5 lid 1 sub b wetsvoorstel). De AP denkt hier – vanwege de (gebleken) kwetsbaarheid[18] - bijvoorbeeld aan DigiD en Mijn Overheid, maar ook – vanwege hun kritische functie - aan de 112-meldkamers.

De AP adviseert te zijner tijd – bij het ontwerpen van de AMvB als bedoeld in artikel 5 wetsvoorstel – te overwegen ook (onderdelen van) de overheid zelf als vitale aanbieder in de zin van artikel 5 lid 1 sub b wetsvoorstel aan te wijzen.

[14] In het wetsvoorstel wordt dit aan elkaar geschreven: digitaledienstverleners.
[15] Cyber Security Raad advies "Naar een landelijk dekkend stelsel van informatieknooppunten" (2017), p. 3.
[16] Cyber Security Raad advies "Naar een landelijk dekkend stelsel van informatieknooppunten" (2017), p. 8.
[17] Gedefinieerd in artikel 4 lid 6 NIB Richtlijn.
[18] CPB Risicorapportage cyberveiligheid economie, p. 5.

VI. Verwerking van persoonsgegevens in het kader van dit wetsvoorstel

1. In de MvT wordt vermeld dat persoonsgegevens worden verwerkt met inachtneming van de AVG.[19] Daaruit zou opgemaakt kunnen worden dat in het kader van de Cybersecuritywet geen persoonsgegevens zullen worden verwerkt die vallen onder het regime van Richtlijn (EU) 2016/680. De AP adviseert u dit nader te adstrueren in de MvT met inachtneming van hetgeen de AP eerder heeft opgemerkt over de reikwijdte van Richtlijn (EU) 2016/680[20].

2. In de uitvoering van dit wetsvoorstel zal vaak gebruik worden gemaakt van namen, emailadressen, wachtwoorden, IP-adressen en andere persoonsgegevens van zowel daders als slachtoffers van cybercrime. Mede vanwege het feit dat het NCSC is ondergebracht bij het ministerie van Veiligheid en Justitie bewegen deze gegevens soms wellicht van het domein van de cybersecurity naar het domein van politie en justitie (en mogelijk weer terug).

   De AP mist aandacht voor dit belangrijke aspect en zou graag de MvT aangevuld zien met een analyse van deze problematiek en met een inschatting van de bijbehorende risico's voor de persoonlijke levenssfeer.

3. Artikel 17 lid 2 wetsvoorstel: ervan uitgaande dat dit artikellid is gebaseerd op artikel 23 lid 1 AVG, dan verplicht artikel 23 lid 2 AVG om - waar van toepassing - specifieke bepalingen op te nemen met betrekking tot ten minste de in artikel 23 lid 2 AVG opgesomde onderdelen. In de toelichting op het wetsvoorstel is niet terug te zien of de wetgever uitdrukkelijk heeft stilgestaan bij de vraag of in dit geval aanleiding bestaat om te voorzien in dergelijke specifieke bepalingen.

4. Daarnaast heeft de AP de volgende vragen, welke in de MvT van een antwoord zouden kunnen worden voorzien.

a. Zijn er buiten de in artikel 18-20 van het wetsvoorstel voorziene gevallen nog andere situaties waarin NCSC persoonsgegevens kan verstrekken aan derden? Zo ja, welke derden zijn dit dan?

b. Artikel 20 wetsvoorstel: betreft de openbaarmaking ook persoonsgegevens? Zo ja, in welke gevallen en om welke persoonsgegevens gaat dat dan?

[19] MvT p. 34.
[20] Advies ten aanzien van het wetsvoorstel inzake de implementatie van Richtlijn (EU) 2016/680 (7 april 2017/z2017-1571).

VII. Diversen/Redactioneel

1. In artikel 2 sub b wordt de minister van V&J – voor wat betreft aanbieders van een essentiële dienst - aangewezen als CSIRT. Dit geldt dus niet voor andere – aangewezen - vitale aanbieders.[21] De achtergrond hiervan is vermoedelijk dat de NIB Richtlijn niet verplicht tot de aanwijzing van een CSIRT voor deze groep aanbieders. Niettemin kan de vraag worden opgeworpen of deze gescheiden aanpak verstandig is. De NIB Richtlijn biedt de mogelijkheid dit anders te regelen (minimumharmonisatie).[22]

2. Artikel 3 lid 2 sub c en artikel 19 lid 2 sub b: "computercrisisteam" is niet gedefinieerd. Zeker omdat in het wetsvoorstel eveneens sprake is van *computer security incident response team* – wat op het eerste gezicht ongeveer hetzelfde lijkt – is de term "computercrisisteam" onduidelijk. Deze term zou daarom moeten worden gedefinieerd.[23]
   Omdat volgens deze bepalingen computercrisisteams worden aangewezen bij regeling van Onze Minister of behorend tot een bij die regeling aangewezen categorie, zou de afbakening van dit begrip voorts pas helder worden in de ministeriële regeling. Dit lijkt onwenselijk.[24]

3. Artikel 7 lid 2 geldt kennelijk niet voor de vitale aanbieders. Dit kan worden verklaard doordat de bepaling een implementatie vormt van artikel 16, eerste lid, van de richtlijn en deze bepaling uit de richtlijn alleen betrekking heeft op digitale dienstverleners. Echter de in artikel 7 lid 2 genoemde aspecten zijn evenzeer relevant voor de vitale aanbieders. De AP adviseert u "van de digitale dienstverlener" in artikel 7 lid 2 te schrappen.

4. Artikel 10 lid 1, aanhef: schrappen "onder a of b".

5. Artikel 10 en 13: definities
   De begrippen "incident" (artikel 10 lid 1 sub a, artikel 13 lid 1), "inbreuk" (artikel 10 lid 1 sub b) en "gebruiker" (artikel 10 lid 4 sub a, artikel 13 lid 2) zijn niet gedefinieerd, terwijl de inhoud van deze begrippen – mede - bepalend is voor de reikwijdte van de meldplichten van artikel 10 en 13.

6. Artikel 11: Zou niet ook de oorzaak van het incident – indien bekend - moeten worden vermeld?

7. Artikel 12 lid 2: Wat is de betekenis van deze bepaling gezien het feit dat ingevolge artikel 10 lid 1 *ook* moet worden gemeld bij de minister van V&J?

8. Artikel 19 lid 2 sub c: geschiedt deze verstrekking ook eigener beweging (dus zonder een verzoek van de AIVD)?

[21] De CSIRT zoals gedefinieerd in artikel 1 – niet zijnde de "CSIRT voor digitale diensten"- lijkt in het wetsvoorstel verder overigens geen rol van betekenis te spelen.
[22] Artikel 3 NIB Richtlijn.
[23] Zie ook Aanwijzing voor de regelgeving 121.
[24] Zie Aanwijzing voor de regelgeving 25.

Datum
25 oktober 2017

Ons kenmerk
z2017-4917

Dictum
De AP adviseert u aan het vorenstaande op passende wijze aandacht te schenken.

De AP verneemt graag op welke wijze u gevolg geeft aan het advies. De AP is beschikbaar indien nadere toelichting is vereist.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Autoriteit Persoonsgegevens,
Voor deze,

Mr. W.B.M. Tomesen
Vicevoorzitter