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 Justitie en Veiligheid
dhr. prof. mr.
Postbus 20301
2500 EH DEN HAAG

Datum	Ons kenmerk	Uw brief van
25 oktober 2021		21 juni 2021
	Contactpersoon	Uw kenmerk

Onderwerp
Wijziging Wbni

Geachte heer ,

Bij brief van 21 juni 2021 is de Autoriteit Persoonsgegevens (AP) op grond van het bepaalde in artikel 36, vierde lid, van de Algemene verordening gegevensbescherming (AVG), geraadpleegd over het concept voor Wijziging van de Wet beveiliging netwerk- en informatiesystemen in verband met de uitbreiding van de bevoegdheid van de Minister van Justitie en Veiligheid om dreigings- en incidentinformatie over de netwerk- en informatiesystemen van niet-vitale aanbieders te verstrekken aan deze aanbieders en aan organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten ten behoeve van deze aanbieders (hierna: het concept).

De AP heeft een aantal opmerkingen over het concept en adviseert daarmee rekening te houden.

Strekking van het concept

Het concept zorgt voor een uitbreiding van de bevoegdheid van het Nationaal Cyber Security Centrum (NCSC) om namens de Minister van Justitie en Veiligheid zogenaamde "andere aanbieders"[1] –

[1] Dit zijn aanbieders, die geen "vitale aanbieder" zijn en evenmin deel uitmaken van de rijksoverheid.
Een "aanbieder" is een "overheidsorganisatie of privaatrechtelijke rechtspersoon die een dienst exploiteert, beheert of beschikbaar stelt" (artikel 1 Wbni). Het begrip kent geen verdere afbakening.
"Vitale aanbieders" zijn aanbieders die diensten aanbieden waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving én daarom door het betrokken vakdepartement zijn aangemerkt als vitale aanbieder. Voorbeelden hiervan zijn een landelijke of regionale aanbieder/distributeur van elektriciteit, een telecomaanbieder en een drinkwaterbedrijf. Deze vitale aanbieders worden dus niet verstaan onder de in het voorstel bedoelde "andere aanbieders".

rechtstreeks of via zogenaamde OKTT's[2] - te informeren over dreigingen en incidenten betreffende hun netwerk- en informatiesystemen. Dit betreft onder andere persoonsgegevens.[3]

Het concept strekt met name tot de volgende aanpassingen van de Wet beveiliging netwerk- en informatiesystemen (verder: Wbni):

a. het in bepaalde gevallen delen van dreigings- en incidentinformatie met "andere aanbieders";
b. het delen van vertrouwelijke herleidbare gegevens[4] met betrekking tot die aanbieders aan OKTT's.

Ad a) In dit kader wordt ook wel gesproken van "restdata" of "bijvangst".[5] Het huidige artikel 3, tweede lid, Wbni regelt dat het NCSC deze informatie, met inbegrip van persoonsgegevens, kan verstrekken aan CSIRT's,[6] computercrisisteams[7] en OKTT's (schakelorganisaties).

De voorgestelde bevoegdheid tot het rechtstreeks verstrekken van restdata aan "andere aanbieders" is beperkt tot bepaalde gevallen:

- het NCSC mag alleen informatie delen met "andere aanbieders" indien er geen schakelorganisatie is die de aanbieder van die informatie kan voorzien;
- er dient sprake te zijn van informatie over een dreiging of incident met (potentiële) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de betrokken aanbieder.[8]

---

[2] Een OKTT is een organisatie die objectief kenbaar tot taak heeft om andere organisaties of het publiek te informeren over hen betreffende digitale dreigingen en incidenten (artikel 3, tweede lid, Wbni). Over OKTT's is in de wetsgeschiedenis van de Wet gegevensverwerking en meldplicht cybersecurity (de voorloper van de Wbni) aangegeven dat de hiervoor bedoelde taak objectief kenbaar kan zijn doordat dit bijvoorbeeld blijkt uit een wettelijk voorschrift of uit de statuten van de organisatie (Kamerstukken II 2015/16, 34388, nr. 3, p. 25 en Kamerstukken II 2015/16, 34388, nr. 6, p. 17). Op dit moment zijn Cyberweerbaarheidscentrum Brainport, de Nationale Beheersorganisatie Internetproviders (NBIP), AbuseHub (een samenwerkingsverband met enkele ISP's, surfnet en SIDN), Cyberveilig Nederland (een samenwerkingsverband van cybersecuritybedrijven), FERM (haven Rotterdam) en Connect2Trust (cros-sectoraal cybersecurity samenwerkingsverband) voorbeelden van krachtens artikel 3, tweede lid, Wbni als zodanig aangewezen OKTT's (ministeriële *aanwijzing*).
Op 1 september 2021 is ook de minister van Economische Zaken en Klimaat (EZK) aangewezen als OKTT (hiervan is geen officiële publicatie beschikbaar). Uit ambtelijk verstrekte informatie van het ministerie van EZK heeft de AP vernomen dat deze aanwijzing zal vervallen zodra het wetsvoorstel Bevordering digitale weerbaarheid bedrijven (Overheid.nl | Consultatie Wet bevordering digitale weerbaarheid bedrijven (internetconsultatie.nl) in werking treedt.
In het concept is overigens geregeld dat de OKTT-aanwijzing voortaan bij ministeriële *regeling* gebeurt.
[3] Zie ook artikel 17 Wbni. Gedacht moet worden aan IP-adressen, domeinnamen en e-mailadressen (van organisaties en/of werknemers) die kwetsbaar zijn voor dan wel getroffen zijn door een digitale aanval, maar ook die van waaruit digitale aanvallen afkomstig zijn.
[4] Dit is een subcategorie van de hiervoor genoemde dreigings- en incidentinformatie.
[5] Deze gegevens noemt men "restdata" of "bijvangst" omdat het gaat om gegevens die het NCSC heeft verkregen in het kader van de uitoefening van de in artikel 3, eerste lid, Wbni bedoelde primaire taakuitoefening (ten behoeven van Rijk en vitale aanbieders), maar die betrekking hebben op netwerk- en informatiesystemen van andere aanbieders dan die deel uitmaken van Rijk en vitaal.
[6] Computer security incident response teams als bedoeld in artikel 1 Wbni.
[7] Niet wettelijk gedefinieerd. Computercrisisteams als bedoeld in de Wbni zijn aangewezen in de Regeling aanwijzing computerteams. Een voorbeeld van zo'n computercrisisteam is de stichting Z-CERT voor de zorgsector.
[8] Daarnaast geldt nog de algemene restrictie dat verstrekking alleen mag ter voorkoming van nadelige maatschappelijke gevolgen in en buiten Nederland (zie het huidige artikel 3, tweede lid, aanhef Wbni).

Ad b) Het huidige artikel 20, tweede lid, Wbni biedt de grondslag voor het NCSC om, zonder instemming van aanbieders, vertrouwelijke gegevens die herleid kunnen worden tot deze aanbieders[9] te verstrekken aan een beperkte kring van organisaties[10]. Met dit wetsvoorstel worden ook OKTT's in deze kring opgenomen, waardoor verstrekking van zulke gegevens straks ook aan OKTT's kan plaatsvinden.

Advies

Strafrechtelijke gegevens?

Het concept geeft het NCSC de taak om "andere aanbieders" te informeren over dreigingen en incidenten betreffende hun netwerk- en informatiesystemen. Dit betreft onder andere IP-adressen van waaruit digitale aanvallen afkomstig zijn.[11] Zulke aanvallen kunnen strafbaar zijn volgens artikel 138ab, 139d en/of 350a Wetboek van Strafrecht (*cybercrime)*. Het is daarom niet uitgesloten dat deze IP-adressen kwalificeren als "persoonsgegevens betreffende [...] strafbare feiten" in de zin van artikel 10 AVG.[12] Dit is extra relevant nu met dit concept deze gegevens ook ter beschikking komen van private partijen. De memorie van toelichting gaat niet in op deze vraag.

De AP adviseert in de memorie van toelichting aan te geven of de hierboven bedoelde IP-adressen moeten worden beschouwd als persoonsgegevens betreffende strafbare feiten in de zin van artikel 10 AVG, en zo ja, welke consequenties de toepasselijkheid van artikel 10 AVG heeft voor de verwerking van deze IP-adressen in het kader van dit wetsvoorstel.

Verstrekking aan "andere aanbieders" onvoldoende afgebakend

Het concept geeft het NCSC de taak om "andere aanbieders" te informeren over dreigingen en incidenten betreffende hun netwerk- en informatiesystemen.

Dit mag alleen indien:

- er geen schakelorganisatie is die de aanbieder van die informatie kan voorzien;
- sprake is van informatie over een dreiging of incident met (potentiële) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de betrokken aanbieder.[13] [14]

Artikel 6, derde lid, AVG geeft aan dat indien een verwerking zijn grondslag vindt in artikel 6, eerste lid, onder c of e, deze verwerking een wettelijke basis moet hebben.[15] In deze wettelijke basis kunnen

[9] Zoals namen van aanbieders.
[10] CSIRT's, AIVD, MIVD, en de in de Regeling aanwijzing computerteams aangewezen computercrisisteams.
[11] Memorie van toelichting, p. 3.
[12] Zie ook N. Falot en C.M. Kroon-Koning, "De verwerking van dreigingsinformatie in het kader van netwerk- en informatiebeveiliging: strafrechtelijke persoonsgegevens in de zin van de AVG?" in *Computerrecht* 2019/4.
[13] Artikel 3, tweede lid, onder e, Wbni.
[14] Zie ook voetnoot 8.
[15] Hoewel de memorie van toelichting zich hierover niet uitspreekt, moet worden aangenomen dat de grondslag voor de verstrekking van NCSC aan de "andere aanbieders" is gelegen in artikel 6, eerste lid, onder e, AVG.

specifieke bepalingen worden opgenomen over "de entiteiten waaraan [...] de persoonsgegevens mogen worden verstrekt".[16]

In dit verband valt op dat het begrip "andere aanbieders" een zeer ruim bereik heeft.[17] De voorwaarde "dat er geen schakelorganisatie is" is dermate fluïde dat deze geen wezenlijke, concrete beperking stelt aan de verstrekkingen door NCSC. Het is namelijk op dit moment niet voorzienbaar hoeveel schakelorganisaties te zijner tijd in functie zullen zijn en of dit een dekkend stelsel van schakelorganisaties zal opleveren. Ten slotte laat de conditie dat sprake moet zijn van (potentiële) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de betrokken aanbieder veel ruimte voor (subjectieve) invulling. Hetzelfde geldt voor de algemene restrictie dat verstrekking alleen mag ter voorkoming van nadelige maatschappelijke gevolgen in en buiten Nederland.[18]

Al met al wordt de kring van ontvangers nauwelijks afgebakend en zijn de voorwaarden waaronder mag worden verstrekt bepaald niet strikt geformuleerd. "Andere aanbieders" zijn in hun omgang met persoonsgegevens bovendien niet, zoals OKTT's, gebonden aan hun wettelijke of statutaire taken en opereren derhalve binnen de ruime doelstelling van de verstrekking zoals verwoord in de memorie van toelichting:

"het nemen van maatregelen om digitale incidenten te voorkomen of te verhelpen en daarmee de continuïteit van hun dienstverlening zo goed mogelijk te waarborgen".[19]

Daarbij komt dat de gegevensverstrekking aan "andere aanbieders" ook wordt bestreken door het wetsvoorstel Bevordering digitale weerbaarheid bedrijven.[20] Dit wetsvoorstel regelt onder andere de taak van de Minister van EZK[21] om niet-vitale bedrijven te informeren en adviseren over digitale dreigingen en incidenten. Omdat "andere aanbieders" ook bedrijven kunnen zijn[22], is op dit punt sprake van overlap met de Wet bevordering digitale weerbaarheid bedrijven.[23]

De AP adviseert de verstrekking aan "andere aanbieders" veel beter af te bakenen. Gezien de overlap met het wetsvoorstel Bevordering digitale weerbaarheid bedrijven adviseert de AP daarbij te overwegen bedrijven[24] uit te zonderen van het begrip "andere aanbieders".

---

[16] Artikel 6, derde lid, AVG.
[17] Geen vitale aanbieder en geen onderdeel van de rijksoverheid. Zie ook voetnoot 1.
[18] Zie ook voetnoot 8.
[19] Memorie van toelichting, p. 2.
[20] Overheid.nl | Consultatie Wet bevordering digitale weerbaarheid bedrijven (internetconsultatie.nl).
[21] In de praktijk is dit het Digital Trust Center (DTC; Home | Digital Trust Center (Min. van EZK)).
[22] Zie voetnoot 1.
[23] Verschil tussen beide wetsvoorstellen v.w.b. persoonsgegevens is dat NCSC ook gegevens van de "aanvaller" (bijv. IP-adres van de hacker) verspreidt, EZK (c.q. DTC) verwerkt alleen persoonsgegevens uit het domein van het "aangevallen" bedrijf (bijv. contactgegevens, een gecompromitteerd account van een medewerker etc. – dus geen IP-adres van de hacker).
[24] in de zin van de Wet bevordering digitale weerbaarheid bedrijven.

Datum
25 oktober 2021

Ons kenmerk

De grondslag van de verwerking door publieke "andere aanbieders"
De memorie van toelichting belicht niet op welke grondslag(en) de verwerking door "andere aanbieders" steunt, terwijl dat in dit geval niet zonder meer helder is.

"Andere aanbieders" kunnen zowel overheidsorganisaties[25] als private partijen zijn.[26] Overheidsorganisaties kunnen de grondslag van artikel 6, eerste lid, onder f, AVG *in het kader van de uitoefening van hun taken* niet gebruiken. De vraag is dan of de informatie over dreigingen en incidenten in dit geval binnen dat kader wordt verwerkt of dat de overheidsorganisatie hier integendeel niet "als overheid" handelt maar "slechts" bezig is een ICT-probleem op te lossen. Het antwoord op deze vraag is bepalend voor de grondslag van de verwerking.

De AP adviseert in de memorie van toelichting aan te geven welke grondslag van toepassing is op de verwerking door publieke "andere aanbieders".

VPN
In de memorie van toelichting is op zeker moment sprake van "kwetsbaarheden in systemen vanwege het gebruik van (versies van) VPN-software".[27] Dit wekt ten onrechte de indruk dat het gebruik van VPN-software als zodanig riskant is. De opmerking in de memorie van toelichting heeft betrekking op een beveiligingsincident met Pulse VPN-software bij onderdelen van het Rijk en bepaalde vitale aanbieders in 2019[28], ontstaan doordat een oudere softwareversie werd gebruikt, die kwetsbaarheden bevatte. Kwetsbaarheden kunnen in iedere soort software voorkomen, en zijn dus niet specifiek voor VPN-software.

De AP adviseert de memorie van toelichting hierop aan te passen.

Openbaarmaking van het advies

De AP is voornemens dit advies na vier weken openbaar te maken op de website www.autoriteitpersoonsgegevens.nl. Behoudens tegenbericht gaat zij ervan uit dat hiertegen geen bezwaar bestaat.

Hoogachtend,
Autoriteit Persoonsgegevens,

Vicevoorzitter

[25] Lagere overheden (zie ook voetnoot 1).
[26] Dit volgt uit de definitie van "aanbieder". Zie ook voetnoot 1.
[27] Memorie van toelichting, p. 4.
[28] Zie Kamerstukken II 2019/20, 26643, nr. 666.

20211027.065.00007

AUTORITEIT
PERSOONSGEGEVENS

PostNL
Port Betaald
Port Payé
Pays-Bas

Postbus 93374, 2509 AJ Den Haag

FMHaaglanden
27 OKT. 2021
Ontvangen

Gezien scankamer
JenV
27 OKT. 2021

RD4CC #X830X0X#00#0000#