AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

De Minister van Justitie en Veiligheid
Mevrouw drs. D. Yeşilgöz-Zegerius
Postbus 20301
2500 EH DEN HAAG

Datum	Ons kenmerk	Uw brief van
20 juni 2024	z2024-013712	14 mei 2024
	Contactpersoon	Uw kenmerk

Onderwerp
Wetgevingstoets concept voor wetsvoorstel Cyberbeveiligingswet (NIS2)

Geachte mevrouw Yeşilgöz,

Bij brief van 14 mei 2024 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 het wetsvoorstel Regels ter implementatie van 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) (hierna: het concept).

De AP heeft enkele aanmerkingen op het concept.

Hoofdlijn

- Het doel van de NIS2-richtlijn is om eenheid en samenhang te brengen in Europees beleid voor netwerk- en informatiebeveiliging, door de digitale paraatheid te vergroten en de gevolgen van cyberincidenten te verkleinen.
- Hiertoe maakt de NIS2-richtlijn, alsook het concept, onder meer onderscheid tussen essentiële entiteiten en belangrijke entiteiten en worden een zorgplicht, een meldplicht en een verplichting tot het verstrekken van informatie opgelegd.
- Het concept wijst een aantal instanties aan die belast zijn met in het concept genoemde taken, in het kader waarvan deze instanties onder meer persoonsgegevens mogen verwerken.
- Het concept is onvoldoende duidelijk over welke persoonsgegevens, waaronder bijzondere categorieën van persoonsgegevens, verwerkt mogen worden.
- Ook bevat het concept geen bewaartermijn en evenmin een delegatiegrondslag om hierover in gedelegeerdere regelgeving regels te stellen.
- Daarnaast is de boetebevoegdheid van de AP niet juist in het concept geïmplementeerd.

Datum
20 juni 2024

Ons kenmerk
z2024-013712

Strekking van het concept

Het concept strekt tot implementatie van Richtlijn (EU) 2022/2555[1] (hierna: NIS2-richtlijn) in Nederlandse wetgeving. Het doel van de NIS2-richtlijn is om eenheid en samenhang te brengen in Europees beleid voor netwerk- en informatiebeveiliging, door de digitale paraatheid te vergroten en de gevolgen van cyberincidenten te verkleinen. Ter implementatie van de NIS2-richtlijn introduceert het concept een nationaal register van entiteiten, beheerd door de minister van Justitie en Veiligheid, waarin essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen dienen te worden opgenomen.[2] Het concept bevat een zorgplicht voor essentiële en belangrijke entiteiten om passende en evenredige technische, operationele en organisatorische maatregelen te nemen om risico's voor de beveiliging van de netwerk- en informatiesystemen die zij gebruiken te beheersen.[3] Verder bevat het concept een aantal verplichtingen op het gebied van governance voor de leden van het bestuur van essentiële en belangrijke entiteiten[4] en introduceert het concept een meldplicht voor significante incidenten.[5] Het concept wijst daarnaast een aantal instanties aan[6], die bepaalde in het concept genoemde taken hebben. Deze instanties zullen bij het uitoefenen van hun taken ook persoonsgegevens verwerken.

Wetgevingstoets

1. Rechtszekerheid

Samenwerking en informatie-uitwisseling
De artikelen 52, eerste en tweede lid, 53, 55, eerste lid, 56 en 57 van het concept bepalen, kort samengevat, dat de in die artikelen genoemde instanties dienen samen te werken voor de doeltreffende en doelmatige uitvoering van hun taken en dat zij daartoe onderling alle daarvoor benodigde gegevens, waaronder persoonsgegevens, uitwisselen. De taken van de betreffende instanties zijn geregeld in hoofdstuk 5 van het concept.

Bijzondere persoonsgegevens
Artikel 64a, tweede lid, van het concept bepaalt dat het verbod om bijzondere categorieën van persoonsgegevens te verwerken, gelet op artikel 9, tweede lid, aanhef en onderdeel g, AVG, niet van toepassing is als het gaat om verwerking door het CSIRT (Computer security incident response team[7]) en

[1] 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).
[2] Artikelen 22 en 45 tot en met 47 van het concept.
[3] Artikel 23 van het concept.
[4] Artikel 26 van het concept.
[5] Artikelen 27 tot en met 31 van het concept.
[6] Te weten het centrale contactpunt (artikel 15 concept), bevoegde autoriteiten (artikel 16 concept), het CSIRT (artikel 17 concept), coördinator bekendmaking kwetsbaarheden (artikel 18 concept) en de cybercrisibeheerautoriteit (artikel 19 concept).
[7] Gernoemd in artikel 10 van de NIS2-richtlijn.

de bevoegde autoriteit voor zover die verwerking noodzakelijk is voor de uitoefening van hun taken op grond van de Cyberbeveiligingswet.

Vertrouwelijke gegevens
Artikel 65 van het concept regelt de mogelijkheid voor de daar genoemde instanties om onder voorwaarden vertrouwelijke gegevens te verstrekken aan elkaar en aan in het artikel genoemde autoriteiten.

Een belangrijk vereiste dat mede voortvloeit uit het evenredigheidsbeginsel en ook in de overwegingen van de AVG wordt aangehaald, is dat een rechtsgrond of wetgevingsmaatregel voor de verwerking van persoonsgegevens (en dus een inbreuk op het recht op bescherming van de persoonsgegevens) voldoende duidelijk en nauwkeurig moet zijn, en dat de toepassing van die rechtsgrond of wetgevingsmaatregel in de praktijk voorspelbaar moet zijn voor degenen op wie deze van toepassing is.
Uit de eis dat een inmenging in de uitoefening van het recht op respect voor het privéleven en de bescherming van persoonsgegevens moet zijn voorzien bij wet, vloeit daarom voort dat die inmenging moet berusten op een naar behoren bekend gemaakt wettelijk voorschrift waaruit de burger met voldoende precisie kan opmaken welke persoonsgegevens met het oog op de vervulling van een bepaalde overheidstaak kunnen worden verzameld en vastgelegd, en onder welke voorwaarden die gegevens met dat doel kunnen worden bewerkt, bewaard en gebruikt. De regeling zelf moet dus voldoende specifiek zijn. Het in de toelichting bij een regeling noemen van voorbeelden van persoonsgegevens waaraan gedacht kan worden bij de betreffende regeling is niet voldoende.

Uit de hiervoor genoemde artikelen betreffende samenwerking en informatie-uitwisseling blijkt niet welke soorten persoonsgegevens kunnen worden uitgewisseld. Het concept bevat ook geen grondslag om dit bij gedelegeerde regelgeving te bepalen.

Uit artikel 64a van het concept is niet op te maken om welke categorieën bijzondere persoonsgegevens het gaat. In het tweede lid is weliswaar bepaald dat bij of krachtens amvb regels kunnen worden gesteld over de verwerking van bijzondere persoonsgegevens; dit is echter niet dwingend voorgeschreven.

Uit artikel 65 van het concept blijkt niet wat precies onder vertrouwelijke gegevens dient te worden verstaan. Dit is ook niet elders in het concept gedefinieerd.

De AP concludeert dat het concept op de hiervoor genoemde punten niet voldoende duidelijk en nauwkeurig is en de toepassing van het concept op deze punten onvoldoende voorspelbaar is, zodat aanpassing van de artikelen 52, eerste en tweede lid, 53, 55, eerste lid, 56, 57, 64a en 65 van de wettekst noodzakelijk is door:

1. in de wettekst een grondslag op te nemen die dwingend voorschrijft om in gedelegeerde regelgeving te bepalen welke soorten persoonsgegevens kunnen worden uitgewisseld ten behoeve van de samenwerking, bedoeld in de artikelen 52, eerste en tweede lid, 53, 55, eerste lid, 56 en 57 van het concept;

2. het tweede lid van artikel 64a van het concept imperatief te formuleren en daarin tevens voor te schrijven dat bij amvb in elk geval wordt bepaald welke categorieën van bijzondere persoonsgegevens noodzakelijk zijn voor de uitoefening van de taken van het CSIRT en de bevoegde autoriteit;
3. in het concept te definiëren wat precies wordt verstaan onder het begrip 'vertrouwelijke gegevens' dan wel in artikel 65 van het concept een grondslag op te nemen die dwingend voorschrijft om in gedelegeerde regelgeving te bepalen welke gegevens dit zijn.

2. Bewaartermijn

In het concept ontbreekt een bepaling over de bewaartermijn van persoonsgegevens die verwerkt worden door de in het concept aangewezen instanties ten behoeve van de uitvoering van hun taken. In par. 6.2.2.2 van de toelichting bij het concept staat dat de Minister van Justitie en Veiligheid in het kader van haar taak als centrale contactpunt telkens zal bekijken of het met het oog op die taak nodig is om de daarvoor van het CSIRT ontvangen persoonsgegevens te bewaren. Ten aanzien van het CSIRT en de bevoegde autoriteiten vermeldt de toelichting dat deze instanties ten behoeve van hun taken ontvangen persoonsgegevens niet langer bewaren dan noodzakelijk. Volgens de Data Protection Impact Assessment (hierna: DPIA) bij het concept is momenteel het uitgangspunt een bewaartermijn van 60 maanden na het afhandelen van het incident of de melding van het incident. Daarbij zou zijn aangesloten bij de praktijk van het melden van een cyberincident op grond van de Wet beveiliging netwerk- en informatiesystemen (Wbni).

Op grond van artikel 5, eerste lid, onderdeel e, AVG mogen persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is. Met het oog hierop dient de verwerkingsverantwoordelijke een termijn vast te stellen voor het wissen van gegevens of voor de periodieke toetsing daarvan.

De AVG bepaalt dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt.[8] Een algemene normstelling zoals deze, betekent dat er moet worden geconcretiseerd voor specifieke gegevensverwerkingen. De AP acht het uit oogpunt van rechtszekerheid in beginsel wenselijk dat de wetgever de bewaartermijn bepaalt als het maken van afwegingen in individuele gevallen niet is aangewezen en een logische bewaartermijn ook niet onmiskenbaar voortvloeit uit de context.

Uit het concept noch uit de toelichting bij het concept blijkt of, en zo ja, welke bewaartermijnen zijn vastgesteld. In het concept is evenmin voorzien in een delegatiegrondslag die het mogelijk maakt om bewaartermijnen in gedelegeerde regelgeving te bepalen. Volgens de DPIA zou een bewaartermijn van 60 maanden noodzakelijk zijn, maar dit is niet in de toelichting onderbouwd.

De AP concludeert dat is aangewezen om met betrekking tot persoonsgegevens die worden verwerkt door de in het concept aangewezen instanties, een bewaartermijn (eventueel in de vorm van maximum) in het concept, of in lagere regelgeving, op te nemen en in de toelichting te onderbouwen. Daarbij dient

[8] Artikel 5, eerste lid, onderdeel e, AVG.

nadrukkelijk aandacht te worden besteed aan de mogelijkheid voor gedifferentieerde bewaartermijnen ten behoeve van de onderscheiden taken van de aangewezen instanties.

3. Internationale doorgifte

In de artikelsgewijze toelichting op artikel 55 van het concept staat onder meer:
"Indien het informatie betreft die ook persoonsgegevens bevatten moet het CSIRT hierbij uiteraard voldoen aan de nationale en internationale regels over de doorgifte van persoonsgegevens aan derde landen, waaronder die van artikel 49 van de Algemene verordening gegevensbescherming. De hierboven genoemde voorbeelden kunnen dan – wanneer het gaat om informatie die ook persoonsgegevens bevat, zoals bijvoorbeeld inloggegevens of mailbestanden– gelden als gewichtige redenen van algemeen belang. Immers, het algemeen belang van Nederland vergt dan, dat kwaadwillende infrastructuur wordt uitgeschakeld of dat ketens gevrijwaard worden van kwaadwillende besmettingen. Het tweede lid van artikel 55 van dit wetsvoorstel strekt tot de implementatie van artikel 10, achtste lid, NIS2-richtlijn en ziet op de samenwerking tussen het CSIRT en een nationaal CSIRT of gelijkwaardig orgaan van een derde land."

Dit lijkt gebaseerd op overweging 45 van de NIS2-richtlijn, waarin, kort gezegd, onder meer staat dat het uitwisselen van persoonsgegevens aan de nationale CSIRT of bevoegde autoriteiten van derde landen mogelijk is, mits wordt voldaan aan de voorwaarden van het Uniegegevensbeschermingsrecht inzake doorgifte van persoonsgegevens aan derde landen, onder meer die van artikel 49 AVG.

In het kader van de uitwisseling van persoonsgegevens met derde landen is echter in de eerste plaats van belang dat wordt nagegaan of er een adequaatheidsbesluit[9] is, waarvan gebruik kan worden gemaakt. Als dat niet het geval is, dient te worden nagegaan of er een grond in artikel 46 AVG is, waarvan gebruik kan worden gemaakt. Dit lijkt aannemelijk, aangezien de uitwisseling zal plaatsvinden tussen publieke instanties binnen de Unie en in derde landen en dan is het mogelijk dat er gebruik kan worden gemaakt van een administratieve regeling ingevolge artikel artikel 46, derde lid, onderdeel b, AVG of van ad hoc contractuele bepalingen als bedoeld in artikel 46, derde lid, onderdeel a, AVG. Pas als geen van deze grondslagen van toepassing is, kan bezien worden of sprake is van één van de uitzonderingsgronden voor specifieke situaties, waarop artikel 49 AVG betrekking heeft.[10]

De AP concludeert dat de huidige tekst in de toelichting bij artikel 55 van het concept ten onrechte de indruk kan wekken dat internationale doorgifte van persoonsgegevens in de zin van dat artikel met name dient plaats te vinden op grond van één van de uitzonderingsgronden in artikel 49 AVG. In de toelichting dient een verduidelijking te worden opgenomen op het punt van de volgorde van grondslagen voor internationale doorgifte conform hetgeen is vermeld in de vorige alinea.

4. Boetebevoegdheid AP

Artikel 52, tweede lid, aanhef en onderdeel b, van het concept bepaalt dat de bevoegde autoriteit, het CSIRT en het centrale contactpunt voor de doeltreffende en doelmatige uitvoering van hun taken

[9] Artikel 45 AVG.
[10] Zie ook de richtsnoeren van de EDPB over artikel 49 AVG en over art. 46 (3)(b) AVG.

samenwerken met onder meer de Autoriteit persoonsgegevens en dat zij alle daartoe benodigde gegevens uitwisselen, waaronder persoonsgegevens. Artikel 52, tweede lid, aanhef en onderdeel b, is volgens de transponeringstabel een implementatie van artikel 35, tweede lid, NIS2-richtlijn. In dat artikellid is, kort samengevat, voorzien in een voorrangsregeling voor het geval terzake van een zelfde gedraging, zowel een NIS2-toezichthouder als de toezichthoudende autoriteit als bedoeld in de AVG bevoegd zijn om een administratieve geldboete op te leggen. Artikel 35, tweede lid, NIS2-richtlijn bepaalt dat in dat geval een toezichthoudende autoriteit als bedoeld in de AVG voor gaat. Dit vloeit voort uit de systematiek van artikel 35 van de NIS2-richtlijn. Artikel 35, eerste lid, van de NIS2-richtlijn ziet op gevallen waarin er mogelijk ook een overtreding van bepalingen van de AVG op het gebied van beveiliging van persoonsgegevens aan de orde is. Indien die overtreding zodanig is dat in voorkomend geval een datalek, als dat zich daadwerkelijk zou voordoen, op grond van de AVG meldingsplichtig zou zijn, dient de AVG-toezichthouder, in casu de AP, te worden ingelicht, zodat deze kan beoordelen of in dat geval een administratieve geldboete op grond van de AVG dient te worden opgelegd. Als de AP voor de betreffende inbreuk een administratieve geldboete oplegt, mag de NIS2-toezichthouder geen geldboete meer opleggen voor dat deel van de overtreding. Deze voorrangsregeling volgt uit artikel 35, tweede lid, NIS2-richtlijn en dient geïmplementeerd te worden in de nationale wetgeving.

Artikel 5:43 van de Algemene wet bestuursrecht (Awb) geeft een algemene regeling voor het geval sprake is van de situatie dat er reeds een bestuurlijke boete is opgelegd aan de overtreder voor dezelfde overtreding. Artikel 5:43 Awb regelt echter niet welk bestuursorgaan er in een bepaald geval voorgaat. Artikel 52, tweede lid, aanhef en onderdeel b, van het concept bepaalt alleen dat er samengewerkt moet worden tussen de NIS2-toezichthouders en de Autoriteit persoonsgegevens als beide bevoegd zijn in geval van dezelfde overtreding, maar niet wie er dan voorgaat bij het opleggen van een bestuurlijke boete.

De AP concludeert dat artikel 35, tweede lid, aanhef en onderdeel b, NIS2-richtlijn niet juist dan wel niet volledig is geïmplementeerd in het concept, zodat aanvulling van de wettekst en de toelichting op dit punt noodzakelijk is.

Werklast AP

De AP voorziet dat het concept zal nopen tot extra inzet. Redengevend hiervoor is dat uit artikel 59, tweede lid, van het concept[11] voortvloeit dat een bevoegde autoriteit, indien zij bij toezicht of handhaving er kennis van krijgt dat een overtreding van de artikelen 23, 27, 28, 29, 30, 31 of 32 van het concept een inbreuk in verband met persoonsgegevens kan inhouden, die op grond van artikel 33 AVG gemeld moet worden, zij de AP daarvan in kennis stelt. De voorziene extra inzet van de AP ziet op:

a. het inrichten van een meldpunt voor NIS2-toezichthouders;
b. het verrichten van een eerste beoordeling van de melding afkomstig van de NIS2-toezichthouder;
c. in overleg met de NIS2-toezichthouder afstemmen en beslissen in welke mate de AP participeert in een onderzoek naar de feiten; en

[11] Implementatie van artikel 35, eerste lid, NIS2-richtlijn.

d. in overleg met de NIS2-toezichthouder afstemmen en beslissen in hoeverre AP als AVG-toezichthouder gebruik wil maken van haar recht op voorrang.

Voor het bepalen van de voor het toezicht van de AP benodigde extra inzet is het van belang dat de AP kennis neemt van de uitvoerings- en handhavingstoetsen (hierna: UHT's) van de NIS2-toezichthouders. Wij verzoeken u dan ook om een afschrift van deze UHT's, zodat de AP kan bepalen wat de gevolgen zijn voor de werkzaamheden van de AP. Mede op basis van deze UHT's zal de AP zelfstandig een UHT opstellen en u deze doen toekomen.

De voorziene extra inzet van de AP voor de bovengenoemde NIS2-taken is nog niet verdisconteerd in de financiering van de AP. Wij gaan er van uit dat de Minister van Justitie en Veiligheid dan wel de Minister voor Rechtsbescherming tijdig zal voorzien in de benodigde financiering voor de uitvoering van de bovenstaande taken van de AP. Een afschrift van deze wetgevingstoets wordt gezonden aan de Minister voor Rechtsbescherming.

Openbaarmaking

Deze wetgevingstoets wordt binnen twee weken op de website van de AP gepubliceerd.

Hoogachtend,
Autoriteit Persoonsgegevens,

Aleid Wolfsen
voorzitter

Datum
20 juni 2024

Ons kenmerk
z2024-013712

-Bijlage

--*--

Toetsingskader AP

De AP beziet of het concept met betrekking tot de verwerking van persoonsgegevens strookt met het Handvest van de Grondrechten van de Europese Unie (EU), de AVG (Verordening 2016/679) of de Richtlijn politie en Justitie (richtlijn 2016/680), de algemene rechtsbeginselen van de EU en het overige relevante recht, waarbij onder meer voldoende aannemelijk moet zijn gemaakt dat voldaan wordt aan het evenredigheidsbeginsel, doordat:

1. het concept geschikt is om de nagestreefde doelstelling van algemeen belang of de bescherming van de rechten en vrijheden van anderen te verwezenlijken (geschiktheid);
2. het doel niet redelijkerwijs even doeltreffend kan worden bereikt op een andere wijze, die de grondrechten van de betrokkenen minder aantast (subsidiariteit);
3. de inmenging niet onevenredig is aan dat doel, wat met name een afweging impliceert van het belang van het doel en de ernst van de inmenging (proportionaliteit);
4. het concept voldoende duidelijk en nauwkeurig is over de reikwijdte en in de toepassing voorspelbaar is (rechtszekerheid);
5. het concept voldoende aangeeft in welke omstandigheden en onder welke voorwaarden persoonsgegevens kunnen worden verwerkt, en aldus waarborgt dat de inmenging tot het strikt noodzakelijke wordt beperkt (inhoudelijke en procedurele waarborgen) en
6. het concept verbindend is naar nationaal recht (verbindendheid naar nationaal recht).

De AP slaat daarbij in het bijzonder acht op de rechten van betrokkenen en de overeenstemming van het concept met artikel 6, eerste en derde lid, en 9, van de AVG (Verordening 2016/679), dan wel 8 en 10 van de Richtlijn politie en Justitie (richtlijn 2016/680) en met de in artikel 5 van de AVG dan wel artikel 4 van de Richtlijn vastgestelde beginselen. Hieruit volgt onder andere dat:

(a) verwerkingen rechtmatig, behoorlijk en transparant moeten zijn ten aanzien van de betrokkene;
(b) dat persoonsgegevens alleen mogen worden verzameld voor welbepaalde, nadrukkelijk omschreven en gerechtvaardigd doeleinden; en
(c) verwerkingen toereikend zijn, ter zake dienend en beperkt moeten zijn tot wat voor de doeleinden noodzakelijk is.

--*--