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
Postbus 20301
2500 EH DEN HAAG

Datum	Ons kenmerk	Uw brief van
10 april 2025	2025-005745	20 februari 2025
	Contactpersoon	Uw kenmerk
		6182251

Onderwerp
Wetgevingstoets concept voor het Cyberbeveiligingsbesluit

Geachte heer Van Weel,

Bij brief van 20 februari 2025 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 een besluit houdende regels ter uitvoering van de Cyberbeveiligingswet (Cyberbeveiligingsbesluit), hierna: 'het concept'.

De AP heeft enkele aanmerking(en) die om aanpassing van het concept vragen.

Hoofdlijn

- Het concept is onvoldoende duidelijk over welke persoonsgegevens verwerkt mogen worden.
- Mogelijk is dat in dit geval niet op voorhand (volledig) mogelijk, maar dan moet dat overtuigend worden onderbouwd.
- In het andere geval dient bij amvb te worden bepaald welke categorieën van (bijzondere) persoonsgegevens noodzakelijk zijn voor de uitoefening van de taken van het CSIRT en de bevoegde autoriteit.
- Het wetsvoorstel moet dan voorzien in een delegatiegrondslag hiervoor.
- Het concept bevat maximale bewaartermijnen die geen effectief maximum zijn doordat de bewaartermijn telkens begint te lopen 'na de laatste bewerking' en zodoende voor veel gegevens telkens automatisch wordt verlengd.

Datum
10 april 2025

Ons kenmerk
2025-005745

Strekking van het concept

Het concept strekt tot implementatie en uitwerking van Richtlijn (EU) 2022/25551 (hierna: NIS2-richtlijn[1]) in Nederlandse wetgeving. De NIS2-richtlijn legt eisen op aan het beheer en de beveiliging die aangewezen entiteiten dienen te waarborgen. De richtlijn legt daarmee een zorgplicht op aan de bepaalde bedrijven en overheidsorganisaties die als speciale entiteiten worden aangewezen in de Cyberbeveiligingswet (Cbw). Het Cyberbeveiligingsbesluit (Cbb) strekt tot de uitwerking van de Cbw, waarmee de NIS2-richtlijn wordt geïmplementeerd.

Wetgevingstoets

De AP benadrukt het toenemende belang van cyberveiligheid- en weerbaarheid in de samenleving. In het bijzonder is cyberveiligheid van belang voor de entiteiten die in uitoefening van hun taak met grote hoeveelheden gevoelige informatie werken. Onder die gevoelige informatie bevinden zich ook persoonsgegevens. Om in lijn met de NIS2-richtlijn de beveiliging van persoonsgegevens te kunnen effectueren, heeft de AP een aantal opmerkingen over het concept.

1. Persoonsgegevens – voldoende duidelijk en nauwkeurig

Het concept bepaalt dat de persoonsgegevens die door het CSIRT en Onze Minister bij of krachtens de wet worden verwerkt, niet langer dan noodzakelijk voor uitoefening van hun bevoegdheden en ten hoogste 60 maanden na de eerste verwerking worden bewaard.[2]

Een rechtsgrond of wetgevingsmaatregel voor de verwerking van persoonsgegevens (en dus een inbreuk op het recht op bescherming van de persoonsgegevens) dient voldoende duidelijk en nauwkeurig te zijn. De toepassing van die rechtsgrond of wetgevingsmaatregel dient in de praktijk voorspelbaar te 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 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 dient tevens voldoende specifiek te zijn, of waar dat omwille van de differentiatie binnen de sectoren niet mogelijk is, dragend te onderbouwen waarom daarvan afgeweken wordt. De AP benadrukt dat het in de toelichting bij een regeling noemen van enkele voorbeelden van persoonsgegevens waaraan gedacht kan worden bij de betreffende regeling niet voldoende is. Uit het concept blijkt onvoldoende welke persoonsgegevens worden verwerkt en voor lange tijd bewaard. Zeker voor potentiële

[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] Artikel 30, eerste lid, van het concept.

bijzondere categorieën van persoonsgegevens is het van belang dat er duiding komt over welke typen gegevens verwerkt en bewaard zullen worden. Uit het concept volgt namelijk dat veel verschillende entiteiten met uiteenlopende en diverse werkzaamheden 'alle nodige' persoonsgegevens kunnen verwerken. De noodzaak om al deze persoonsgegevens te verwerken, zonder nadere uitwerking of specificering van welke gegevens dit redelijkerwijs kunnen zijn, is niet van dragende onderbouwing voorzien. De AP is van mening dat onduidelijkheid omtrent alle aan verwerking onderhevige persoonsgegevens opgehelderd moet worden, niet slechts waar het bijzondere persoonsgegevens en/of de uitwisseling van persoonsgegevens in samenwerkingsverband betreft. Het is denkbaar dat de taakuitoefening van een bestuursorgaan in een bepaald geval dermate breed en onvoorspelbaar is dat nadere duiding van de aard van de bijzondere categorieën van persoonsgegevens vooraf niet mogelijk is. In dergelijke - zeldzame - gevallen moet uit de toelichting blijken dat dat het geval is en waarom dat het geval is. De toelichting lijkt een begin te maken aan een dergelijke verantwoording, maar deze is volgens de AP niet voldoende richtinggevend. Het ligt voor de hand om aan de ene kant de aan verwerking onderhevige bijzondere categorieën van persoonsgegevens bij amvb te beperken tot het volstrekt noodzakelijke, of anderzijds in de toelichting te verantwoorden waarom concretisering van de categorieën persoonsgegevens niet mogelijk is en daarbij concretere voorbeelden te noemen. De AP sluit daarbij aan op het reeds gepubliceerde advies van de Raad van State met betrekking tot de Cyberbeveiligingswet.[3]

In het verlengde van bovenstaande verwijst de AP naar het wetgevingsadvies van 20 juni 2024, waarin de AP er eveneens op wijst dat in een delegatiegrondslag voor de verwerking voorzien dient te worden.[4] De AP benadrukt dat uit de voorliggende en eerder ontvangen stukken geen delegatiegrondslag blijkt voor het verwerken en bewaren van persoonsgegevens, waardoor zij niet na kan gaan of aan deze opmerking gehoor is gegeven.

De AP concludeert dat de te verwerken persoonsgegevens waar mogelijk in de wettekst gespecificeerd dienen te worden, of dat verduidelijking en onderbouwing in de toelichting nodig is.

2. Bewaartermijnen

Het concept bevat een uitzondering op het eerste lid voor de persoonsgegevens die worden verwerkt in het kader van het nationaal register, bedoeld in artikel 43 Cbw.[5] Voor deze persoonsgegevens geldt een maximale bewaartermijn van 60 maanden na de *laatste* wijziging van de betreffende persoonsgegevens, in afwijking van de andere leden van het artikel waar de termijn uiterlijk 60 maanden na de *eerste* verwerking betreft.

Volgens de nota van toelichting is het de verwachting dat het register steeds aangepast of bijgewerkt wordt zodat deze gegevens in de praktijk oneindig bewaard worden.[6] De maximale bewaartermijn van 60 maanden begint voor veel van deze persoonsgegevens immers steeds opnieuw te lopen, waardoor de

[3] Afdeling Advisering Raad van State, Cyberbeveiligingswet (W16.24.00336/II), 19 februari 2025, p. 6 en 7.
[4] Autoriteit Persoonsgegevens, wetgevingsadvies Cybersecuritywet, 20 juni 2024, p. 4.
[5] Artikel 30, tweede lid, van het concept.
[6] Concept memorie van toelichting, p. 19.

termijn geen effectieve waarborg meer is. Om wetgeving en de daaruit voortvloeiende uitvoeringsconsequenties toekomstbestendig te maken, zijn aanvullende criteria of waarborgen nodig die voorkomen dat persoonsgegevens potentieel oneindig bewaard worden. Uit het concept blijken geen voorafgaande waarborgen dat deze noodzakelijkheidsafweging correct toegepast wordt. Een verplichting tot periodieke evaluatie of het opstellen van beleid kan een uitkomst bieden. Daartoe kan men denken aan waarborgen in de vorm van 'privacy by design'.[7]

Bovendien heeft de AP in haar eerder aangehaalde advies van 20 juni 2024 de noodzaak aangegeven om nadrukkelijk aandacht te besteden aan de mogelijkheid voor gedifferentieerde bewaartermijnen ten behoeve van de onderscheiden taken van de aangewezen instanties. Het concept beperkt de bewaartermijn tot het noodzakelijke, doch uiterlijk 60 maanden na de eerste verwerking. Uit het concept volgt dat de noodzakelijkheidsafweging per entiteit dient plaats te vinden. Voorstelbaar is dat niet voor alle taken dezelfde bewaartermijn noodzakelijk zal zijn. Het concept houdt nog geen rekening met differentiatie in onderscheiden taken', waartoe onderbouwing in de toelichting geboden is.

De AP concludeert dat de in het concept opgenomen maximale bewaartermijn niet effectief is voor het tijdig verwijderen van persoonsgegevens zodat aanpassing van de wettekst van artikel 30 tweede lid van het concept nodig is.

Werklast AP

Aannemelijk is dat het concept de AP zal nopen tot extra inzet. Zie hiervoor de reeds gedane oproep in de wetgevingstoets van 20 februari 2024. Deze voorziene extra inzet is nog niet verdisconteerd in de financiering van de AP. Dit zal voorafgaand aan inwerkingtreding in overleg met de Minister voor Rechtsbescherming - als verantwoordelijke voor de begroting ten laste waarvan de AP wordt gefinancierd - moeten worden geadresseerd. Om die reden wordt wederom afschrift van deze wetgevingstoets gezonden aan de Staatssecretaris voor Rechtsbescherming.

Openbaarmaking

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

Hoogachtend,
Autoriteit Persoonsgegevens,

Aleid Wolfsen
voorzitter

-Bijlage

[7] Stcrt. 2013, 5174.

--*--

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*.

--*--