Advies nr. 102/2019 van 5 juni 2019

Betreft: Ontwerp van koninklijk besluit tot uitvoering van de wet tot vaststelling van een kader voor de beveiliging van netwerk –en informatiesystemen van algemeen belang voor de openbare veiligheid, en van sommige bepalingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van kritieke infrastructuren (CO-A-2019-115)

De Gegevensbeschermingsautoriteit (hierna "de Autoriteit");

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit,* inzonderheid op artikel 23 en 26 (hierna "WOG");

Gelet op de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op het verzoek om advies van de Eerste Minister, ontvangen op 10 april 2019;

Gelet op het verslag van Mevrouw Alexandra Jaspar, Directeur van het Kenniscentrum van de Gegevensbeschermingsautoriteit;

Brengt op 5 juni 2019 het volgend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. De Eerste Minister verzocht op 10 april 2019 het advies van de Autoriteit over een ontwerp van koninklijk besluit *tot uitvoering van de wet tot vaststelling van een kader voor de beveiliging van netwerk –en informatiesystemen van algemeen belang voor de openbare veiligheid*, *en van sommige bepalingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van kritieke infrastructuren* (hierna "het Ontwerp").

2. Betreffende een ontwerptekst van de wet *tot vaststelling van een kader voor de beveiliging van netwerk –en informatiesystemen van algemeen belang voor de openbare veiligheid* (hierna "de wet") verleende de Autoriteit reeds advies nr. 84/2018[1]. De wet beoogde de omzetting van de Europese Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 *houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk –en informatiesystemen in de Unie*. Deze richtlijn heeft met name tot doel ervoor te zorgen dat technische –en organisatorische beveiligingsmaatregelen worden genomen door de aanbieders van essentiële diensten en door digitale dienstverleners om incidenten te voorkomen of de impact ervan te beperken, teneinde de continuïteit van deze diensten te waarborgen. In dezelfde geest heeft de in deze richtlijn vervatte meldingsplicht van incidenten – die door middel van de wet in het Belgisch recht geïmplementeerd werd – betrekking op de incidenten die een aanzienlijke impact hebben op de verleende diensten.

3. Het Ontwerp heeft voornamelijk tot doel om

- het algemene kader voor meldingen van beveiligingsincidenten in de zin van de wet vast te stellen,
- de 'bevoegde autoriteiten' waarvan sprake in de wet[2] aan te wijzen en
- de algemene certificeringsvoorwaarden te bepalen voor de instellingen die de externe audits van de aanbieders van essentiële diensten moeten uitvoeren.

---

[1] https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/advies_84_2018.pdf

[2] Ter illustratie:

-artikel 7, §1, van de wet: *"De Koning wijst de autoriteit aan die, als nationale autoriteit, belast is met de opvolging en coördinatie van de uitvoering van deze wet."*

-artikel 10, §1, van de wet: *"De Koning wijst, bij een besluit vastgesteld in de Ministerraad, de autoriteit aan die belast is met de actualisering van de bestaande nationale strategie voor de beveiliging van netwerk –en informatiesystemen."*

(Zie ook randnummer 3 van advies nr. 84/2018).

II. ONDERZOEK VAN DE ADVIESAANVRAAG

4. In haar advies nr. 84/2018 wees de Autoriteit er reeds op dat er in de praktijk tal van raakvlakken zullen opduiken tussen de bepalingen in de wet en de regels inzake dataprotectie. Alle actoren die onderworpen zijn aan de bepalingen in de wet dienen met name – voor zover zij ook persoonsgegevens verwerken – tegelijk rekening te houden met de AVG en haar uitvoeringswetten[3]. Dit geldt bijvoorbeeld ook voor wat betreft de melding van 'veiligheidsincidenten' in de zin van de wet en 'inbreuken in verband met persoonsgegevens' in de zin van de AVG. De Autoriteit maakt daarom vooreerst van de gelegenheid gebruik om te pleiten voor een duidelijke communicatie hieromtrent[4] op de website van het gemeenschappelijk meldingsplatform voor veiligheidsincidenten dat ingevolge het Ontwerp zal gecreëerd worden.

5. Daarnaast neemt de Autoriteit akte van de regeling in het Ontwerp voor de melding van veiligheidsincidenten in de zin van de wet. Hoofdstuk 3 (artikelen 4 t.e.m. 9) van het Ontwerp handelt met name over de "Melding en verwerking van incidenten" en Hoofstuk 4 (artikel 10) van het Ontwerp over de "Vrijwillige meldingen". Art. 6, § 1, van het Ontwerp bepaalt dat de melding van veiligheidsincidenten in de zin van de wet via het gemeenschappelijk meldingsplatform dient te gebeuren en dit op basis van een formulier dat door het Computer Security Incident Response Team wordt opgesteld. De tweede paragraaf van artikel 6 van het Ontwerp voorziet tegelijk in een uitzonderingsregeling voor wat betreft de melding van inbreuken van persoonsgegevens[5]. Laatstgenoemde meldingen worden op basis van deze bepaling met name onderworpen aan de AVG en aan de regels die door de Autoriteit worden opgelegd.

6. De Autoriteit beoordeelt deze uitzonderingsregeling voor de melding van inbreuken van persoonsgegevens positief en zij pleit er tegelijk voor om aan artikel 6, §2, van het Ontwerp een meer algemene draagwijdte te geven, aangezien deze bepaling in haar huidige opbouw enkel in een afwijking lijkt te voorzien op de eerste paragraaf van artikel 6 van het Ontwerp en niet op de andere bepalingen van het Ontwerp. De afwijkende regels voor de melding van inbreuken in verband met persoonsgegevens in de zin van de AVG zouden echter voor de volledige Hoofdstukken 3 & 4 van het Ontwerp moeten gelden, omdat deze hoofdstukken –

---

[3] Randnummers 6 & 7 van advies nr. 84/2018.

[4] Belangrijk punt dat in deze communicatie zou moeten onderlijnd worden betreft het feit dat het de verantwoordelijkheid van de verwerkingsverantwoordelijke betreft om te beslissen bij welke instantie(s) hij een melding doet en bij welke niet (zie randnummer 6 van advies nr. 84/2018).

[5] *"Art. 6. §1. De melding gebeurt via het meldingsplatform met behulp van het formulier voor het melden van incidenten dat is opgesteld door het nationale CSIRT. (…)*

§2. Er wordt afgeweken van paragraaf 1 voor de melding van inbreuken in verband met persoonsgegevens die onderworpen zijn aan de wettelijke regels of de regels opgelegd door de toezichthoudende autoriteit (…)".

naast artikel 6 van het Ontwerp – ook andere bepalingen bevatten waarin regelingen worden getroffen betreffende de melding van veiligheidsincidenten in de zin van de wet[6] en het dient duidelijk te zijn dat deze meldingen geheel los staan van de melding van inbreuken in verband met persoonsgegevens in de zin van de AVG.

7. Een dergelijke verruiming van de draagwijdte van artikel 6, §2, van het Ontwerp zou bijvoorbeeld kunnen gerealiseerd worden door de bewoordingen van deze bepaling ruimer te formuleren (met name door de woorden “paragraaf 1” te vervangen door “dit hoofdstuk”) én door deze bepaling telkens in een apart artikel in het begin van Hoofdstuk 3 en in het begin van Hoofdstuk 4 van het Ontwerp op te nemen.

OM DEZE REDENEN

- adviseert de Autoriteit om een duidelijke communicatie op de website van het gemeenschappelijk meldingsplatform te plaatsen, betreffende het onderscheid tussen de verplichtingen die de wet oplegt en de verplichtingen die uit de AVG voortvloeien (randnummer 4).

- oordeelt de Autoriteit dat de volgende aanpassing aan het Ontwerp zich opdringt: de uitzonderingsregeling voor de melding van inbreuken van persoonsgegevens niet beperken tot artikel 6, maar uitbreiden tot de volledige hoofdstukken 3 & 4 van het Ontwerp (randnummers 6-7).

(get.) An Machtens
Wnd. Administrateur

(get.) Alexandra Jaspar
Directeur van het Kenniscentrum

[6] Zie bv. artikel 7 van het Ontwerp.