



Advies 144/2018 van 19 december 2018

Betreft: Ontwerp van koninklijk besluit betreffende de noodplanning en het beheer van noodsituaties op het gemeentelijk en provinciaal niveau en betreffende de rol van de burgemeesters en de provinciegouverneurs in geval van crisisgebeurtenissen en -situaties die een coördinatie of een beheer op nationaal niveau vereisen. (CO-A-2018-159)

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 de "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 (algemene verordening gegevensbescherming)* (hierna AVG)

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 heer Jan Jambon, Minister van Veiligheid en Binnenlandse Zaken, ontvangen op 6 november 2018;

Gelet op de bijkomende informatie ontvangen op 19 november 2018;

Gelet op het verslag van de heer Willem Debeuckelaere;

Brengt op 19 december 2018 het volgend advies uit:

I. ONDERWERP EN CONTEXT VAN DE AANVRAAG

1. De Minister van Veiligheid en Binnenlandse Zaken (hierna "de aanvrager") vraagt het advies van de Autoriteit over de artikelen 5 tot 7 van zijn ontwerp van koninklijk besluit (KB) betreffende de noodplanning en het beheer van noodsituaties op het gemeentelijk en provinciaal niveau en betreffende de rol van de burgemeesters en de provinciegouverneurs in geval van crisisgebeurtenissen en -situaties die een coördinatie of een beheer op nationaal niveau vereisen.
2. Het ontwerp van KB verplicht de burgemeesters en de provinciegouverneurs noodplannen op te stellen die onder meer de contactgegevens bevatten van de personen die betrokken zijn bij het beheer en de preventie van noodsituaties¹. Volgens het verklarend document bij het ontwerp dat door de aanvrager werd meegedeeld, kan het gaan om natuurlijke personen en meer specifiek om personen die tewerkgesteld zijn bij (vrije vertaling) "*openbare overheden en diensten betrokken bij het beheer van noodsituaties, de opvangcentra, de verantwoordelijken van de instellingen aan de bron of in de omgeving van een bijzonder risico*" en ook de adressen en telefoonnummers van privé-instituten die over expertise beschikken met betrekking tot een bijzonder risico of nog de leveranciers van drinkwater, gas, elektriciteit, vervoer, werken, civiele techniek.

II. Onderzoek

3. Iedere wetgeving die voorziet in verwerkingen van persoonsgegevens moet beantwoorden aan de gebruikelijke kwaliteitscriteria uitgevaardigd door de rechtspraak zodat de betrokkenen van wie gegevens worden verwerkt, zich bij het lezen ervan een duidelijk beeld kunnen vormen van de verwerkingen die met hun gegevens zullen worden uitgevoerd. Daartoe moet zij onder meer nauwkeurig het/de concrete of operationele doeleinde(n) beschrijven van de door de wetgeving omkaderde verwerking, de aard van de gegevens die worden verwerkt, de categorieën betrokkenen van wie de gegevens worden verwerkt, de categorieën ontvangers aan wie de gegevens desgevallend worden meegedeeld en de doeleinden waarvoor deze mededelingen plaatsvinden, de opslagperiodes alsook alle maatregelen die ertoe strekken een behoorlijke en rechtmatige verwerking van de persoonsgegevens te waarborgen.
4. Artikel 5 van het ontwerp bepaalt « *deze nood- en interventieplannen (ANIP) bevatten minimaal:*

¹ Het begrip noodsituatie wordt in artikel 1, 3° van het ontwerp KB gedefinieerd als: "elke gebeurtenis die schadelijke gevolgen voor het maatschappelijke leven veroorzaakt of kan veroorzaken, zoals een ernstige verstoring van de openbare veiligheid, een ernstige bedreiging ten opzichte van het leven of de gezondheid van personen en/of ten opzichte van belangrijke materiële belangen, en waarbij de coördinatie van de bevoegde actoren, inclusief de disciplines, is vereist om de dreiging weg te nemen of om de nefaste gevolgen van de gebeurtenis te beperken".

1° de algemene inlichtingen betreffende de betrokken provincie of gemeente, namelijk:

a) de contactgegevens van de operationele en beleidsdiensten, de betrokken overheden, de gespecialiseerde diensten, de informatiecentra en de deskundigen; (...) »

5. Uit de bijkomende informatie die werd verkregen van de afgevaardigde ambtenaar blijkt dat onder (vrije vertaling) "*repertorium van de operationele en strategische diensten van de betrokken overheden*", dient te worden verstaan "de contactgegevens van de operationele en administratieve verantwoordelijken (naam, functie, telefoon, fax, gsm, e-mail, contacturen)". Gelet op wat voorafgaat dient de tekst van deze bepaling herzien te worden om
- a. eerst en vooral het concrete en operationele doeleinde te preciseren van deze verplichte vermelding in de ANIP en vervolgens,
 - b. de categorieën van persoonsgegevens te preciseren die moeten worden vermeld en dit aangezien de van de afgevaardigde verkregen bijkomende informatie niet wordt weerspiegeld in de ontwerp tekst,
 - c. ook zullen de categorieën betrokkenen² worden gepreciseerd van wie de contactgegevens moeten worden vermeld en het begrip « *betrokken overheden* » zal op nuttige wijze worden vervangen door het begrip overheden waarvan de opdracht van openbare dienst bestaat uit het beheer van noodsituaties.

Zonder deze preciseringen zal het de verwerking niet alleen ontbreken aan transparantie en voorzienbaarheid zoals vereist door de rechtspraak, maar het verplichte karakter van deze vermelding in de ANIP zal er worden door aangetast en het objectief van de auteur van het KB negatief beïnvloeden. Deze laatste mag niet uit het oog verliezen dat deze verduidelijken moeten plaatsvinden in overeenstemming met het beginsel van de minimalisering van gegevens (art. 5.1.c AVG) dat vereist dat de verwerkte persoonsgegevens toereikend, ter zake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de doeleinden waarvoor ze werden ingezameld.

6. Bovendien vestigt de Autoriteit de aandacht op het feit dat niet noodzakelijk persoonsgegevens moeten worden verwerkt om zich ervan te verzekeren dat de *ad hoc* personen kunnen worden gecontacteerd wanneer zich een noodsituatie voordoet. Generieke contactadressen (in de aard van contactcrisismanagement@provincie.be, contactcrisisbrandweer@gemeente.be) kunnen worden gecreëerd om deze rol te vervullen. Een dergelijke werkwijze laat toe te verhelpen aan het verloop van het personeel, hun onbeschikbaarheid wegens ziekte of verlof en aan de noodzaak om de gegevens voortdurend bij te werken zonder te spreken over het feit dat het voor sommige soorten personen, betrokken bij het beheer van sommige specifieke noodsituaties (bijvoorbeeld personen gespecialiseerd in het beheer van terroristische aanslagen), het voor de bescherming

² In elk geval, in toepassing van het beginsel van minimalisering van gegevens dienen de aangewezen personen deze te zijn voor wie uit hun functie blijkt dat zij moeten kunnen gecontacteerd worden ingeval een noodsituatie zich voordoet in de mate dat hun functie/opdracht verbonden is aan het beheer van risico's/noodsituaties.

van hun eigen persoon opportuun kan zijn dat hun identiteit niet wordt opgenomen in een dergelijk plan of gecentraliseerd in een register. Een dergelijke werkwijze vereist dat de bevoegde overheden verplicht worden toe te zien op de bijwerking van hun generiek adressenbestand (of generieke contacttelefoonnummers) om ervoor te zorgen dat hun personeelsleden belast met het dit crisisbeheer wel degelijk de e-mails (of tel.) ontvangen die aan deze adressen worden verstuurd. In toepassing van het beginsel van minimalisering van gegevens beveelt de Autoriteit de auteur van het ontwerp van KB aan om in zijn tekst de vermelding van dit type generieke adressen te voorzien alsook de verplichte bijwerking, ten minste voor de personen van wie de specifieke functie of expertise het nemen van maatregelen vergen voor het beschermen van hun eigen persoon.

7. Betreffende het begrip deskundige bedoeld in artikel 5.1.a) van het ontwerp KB, gaat het, volgens de bijkomende inlichtingen verkregen van de afgevaardigde van de Minister om (vrije vertaling) *"personen die ingevolge hun kennis over een of meerdere aspecten van strategisch- of operationeel crisisbeheer of over een specifiek risico, in staat zijn nuttige informatie te verstrekken voor de te nemen beslissingen inzake crisisbeheer"*. Volgens diezelfde bijkomende inlichtingen kunnen deze deskundigen deel uitmaken van de diensten van de gemeenten of provincies of nog afkomstig zijn uit de privésector (universiteitsprofessoren, persoon van een buitenlandse dienst aanwezig ter ondersteuning van de bevoegde overheden,...) Het ontwerp van KB noopt in dit verband tot de volgende twee opmerkingen:
 - a. Eerst en vooral, in het licht van de voormelde criteria inzake de kwaliteit van wetten, dient het begrip deskundige bedoeld in artikel 5.1.a) van het ontwerp KB, te worden gedefinieerd om nauwkeurig te kunnen worden bepaald.
 - b. Vervolgens, betreffende de deskundigen die geen opdracht van openbare dienst vervullen waardoor zij moeten kunnen gecontacteerd worden in geval van een noodsituatie of voor de preventie van dit soort situatie, dient in het beschikkend gedeelte te worden gepreciseerd dat de vermelding van hun contactgegevens slechts gebeurt nadat deze laatsten specifiek in detail werden geïnformeerd over de verwerking van de hen betreffende gegevens in dit raam en de hiermee verbonden verwerkingen (vermelding in het nationaal veiligheidsportaal Incident & Crisis Management dat ter beschikking wordt gesteld van de overheden) en dat men hen de mogelijkheid heeft geboden zonder motief af te zien van deze vermelding (opt out). Deze opt-out vormt een passende maatregel om zich te verzekeren van de relevantie van de verwerking van hun gegevens in dit raam (zich bij hen vergewissen dat zij wel degelijk deskundig zijn voor het beheer van het bedoelde risico,...)
8. Artikel 6 van het ontwerp KB bepaalt *« De Bijzondere nood-en interventieplannen (BNIP) omvatten ten minste:*

1° de beschrijving van het betrokken risico en de bepaling van de noodplanningszone(s);

2° de gegevens van de actoren die specifiek betrokken zijn bij het risico;

3° ... »

9. Vanuit eenzelfde redenering die werd gevolgd in de vorige opmerkingen, zal het begrip "de actoren die specifiek betrokken zijn bij het risico", bedoeld in artikel 6, §1, 2° van het ontwerp KB, eveneens moeten gedefinieerd worden in het ontwerp van KB om de nauwkeurige en duidelijke bepaling van deze categorieën natuurlijke personen te verzekeren in toepassing van het beginsel van minimalisering van gegevens. Op basis van welke criteria kan een actor betrokken zijn bij een risico (wegens zijn opdracht van openbare dienst en het feit dat hij tussenkomt bij de preventie en het beheer van dit risico? Wegens zijn aanwezigheid in een risicozone en zijn statuut van potentieel slachtoffer?...). Voor het overige wordt verwezen naar de voorgaande opmerkingen over het gebruik van generieke contactadressen.

10. Artikel 7 van het ontwerp KB bepaalt « *§1 De bevoegde overheden bezorgen, ieder wat hen betreft, het NIP (Nood- en interventieplan) aan de overheden, diensten en personen die erin zijn opgesomd als bestemmingen, met name via het nationaal veiligheidsportaal. § 2. De bestemmingen bedoeld in § 1 van dit artikel moeten elke wijziging van de hen betreffende gegevens onmiddellijk aan de betrokken bevoegde overheid meedelen, met name via het nationaal veiligheidsportaal.* »

11. Uit de bijkomende informatie, verkregen van de afgevaardigde van de Minister blijkt dat de formulering van ontwerpartikel 7 § 1 moet worden herzien. Volgens deze informatie dient het NIP door de bevoegde overheid te worden meegedeeld aan de actoren van het crisisbeheer die een rol te vervullen hebben in het betrokken plan en bijgevolg dienen te worden ingelicht. De formulering van deze bepaling van het ontwerp dient te worden herzien opdat de details van deze gegevensmededelingen hierin duidelijk worden bepaald.

12. Bovendien blijkt uit het inleidend document bij de adviesaanvraag dat de noodplannen en de contactgegevens van de sleutelactoren bij noodsituaties, gecentraliseerd zijn in een beveiligd ICMS-portaal (Incident & crisis management system) dat op 1 januari 2017 werd opgericht bij de FOD Binnenlandse Zaken (AD Crisiscentrum) en tot doel heeft de uitwisseling van informatie toe te laten tussen alle bij de noodplanning en crisisbeheer betrokken partners en dit zowel in de planningsfase als tijdens noodsituaties. De auteur van het ontwerp van KB zal ervoor zorgen dat deze centralisatie en gegevensuitwisselingen eveneens blijken uit de formulering van artikel 7 van het ontwerp teneinde een goede graad van voorzienbaarheid te waarborgen voor deze gegevensverwerkingen. Er zal eveneens melding worden gemaakt van het concrete en

operationele doeleinde van dit beveiligde portaal, van de bewaartermijn van de hierin opgenomen persoonsgegevens en van de verwerkingsverantwoordelijke van dit portaal.

13. Betreffende dit beveiligde ICMS-portaal, verwijst het hoofdstuk "gegevensbescherming" van het inleidend document bij de adviesaanvraag, dat aan de Gegevensbeschermingsautoriteit werd gericht, naar het feit dat het behoud en de vermelding van de contactgegevens van alle personen betrokken bij het beheer van crisis- en noodsituaties, respectievelijk is onderworpen aan het niet-uitoefenen van hun opt-out of hun voorafgaande toestemming en dit twee maal per jaar. Er wordt eveneens verduidelijkt dat hun gegevens zullen worden geschrapt binnen de maand nadat zij hebben meegedeeld dat zij wensen dat deze zouden worden verwijderd. In dit verband merkt de Gegevensbeschermingsautoriteit op dat de invoering van dit soort portaal strookt met de opdrachten van openbare dienst van het coördinatie- en Crisiscentrum van de regering, opgericht binnen de FOD Binnenlandse Zaken bij koninklijk besluit van 18 april 1988³. Hieronder bevinden zich immers « *op bestendige wijze de informatie die betrekking heeft op zijn bevoegdheden, te verzamelen en te analyseren, en de verantwoordelijke personen en diensten in te lichten over nationale crisissituaties⁴ of over gebeurtenissen die tot dergelijke toestand kunnen leiden en de nodige infrastructuur en middelen ter beschikking te stellen van de bevoegde overheden voor de beheersing van een nationale crisis, meer bepaald de coördinatie, de voorbereiding van beslissingen, de eventuele uitvoering en de opvolging ervan te verzekeren* » (art. 3 van het voormeld KB van 18/04/1988). Het is dus in uitvoering van zijn openbare dienstverplichtingen (art. 6.1.e van de AVG) dat het Crisiscentrum van de FOD Binnenlandse Zaken dit ICMS-portaal opricht. Het kan hierin dus legitiem persoonsgegevens integreren van personen die een opdracht van openbare dienst vervullen in verband met crisis- of noodsituaties of de preventie van dergelijke situaties, zonder hen hiertoe voorafgaand hun toestemming te vragen maar vanzelfsprekend wel met vervulling van alle door de AVG opgelegde verplichtingen (waaronder de kennisgeving aan de betrokkenen conform de artikelen 13 of 14 AVG al naargelang het gaat om gegevens die rechtstreeks werden verkregen bij de persoon van wie de gegevens al dan niet worden vermeld) en de goedkeuring van specifieke maatregelen als waarborg voor de bescherming van de contactpersonen. Het is pas wanneer in dit portaal gegevens worden vermeld van personen die niet een dergelijke opdracht van openbare dienst vervullen, dat de Gegevensbeschermingsautoriteit oordeelt dat hen een opt-out mogelijkheid als waarborgmaatregel moet worden geboden (cf. supra).
14. Aangaande artikel 7, § 2 van het ontwerp, dat de personen van wie de gegevens worden opgenomen in het nationaal veiligheidsportaal verplicht elke wijziging van de hen betreffende

³ Koninklijk besluit van 18 april 1988 tot oprichting van het coördinatie- en Crisiscentrum van de regering

⁴ Volgens dit KB, is een crisis nationaal "wanneer de bedreiging op het nationaal grondgebied ontstaat of met voornamelijk nationale middelen moet bestreden worden"

gegevens mee te delen, vestigt de Gegevensbeschermingsautoriteit de aandacht van de FOD Binnenlandse Zaken op het feit dat hij, als verwerkingsverantwoordelijke van het ICMS-portaal, in toepassing van artikel 5.1.d van de AVG, verplicht is alle redelijke maatregelen te nemen om zich te verzekeren van de juistheid en de bijwerking van de in het portaal opgenomen persoonsgegevens⁵.

15. De Gegevensbeschermingsautoriteit vestigt eveneens de aandacht van de FOD Binnenlandse Zaken op het feit dat de artikelen 5.1.f en 32 AVG hem verplichten het ICMS portaal te parametriseren zodat, door het nemen van passende technische of organisatorische maatregelen, gewaarborgd is dat de persoonsgegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

16. Artikel 32 AVG wijst in dit verband op een aantal voorbeeldmaatregelen om, waar passend, een op het risico afgestemd beveiligingsniveau te waarborgen:
 - de pseudonimisering en versleuteling van persoonsgegevens;
 - het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen te garanderen;
 - het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
 - een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

17. Voor de concrete uitwerking hiervan wijst de Autoriteit op de aanbeveling⁶ ter voorkoming van gegevenslekken en op de referentiemaatregelen⁷ die bij elke verwerking van persoonsgegevens in acht zouden moeten worden genomen. Aangezien bovendien het ICMS-portaal toegankelijk is en bevoorradat wordt door alle actoren van het crisisbeheer, zowel op gemeentelijk als nationaal niveau, onderstreept de Autoriteit ook het belang van een behoorlijk gebruikers- en toegangsbeheer⁸.

⁵ Dit zonder afbreuk te doen aan het feit dat de gemeenten en provincies beschouwd kunnen worden als verwerkingsverantwoordelijken van hun eigen veiligheidsplan wat betreft de persoonsgegevens die zij verzamelen om dit op te stellen.

⁶ Aanbeveling uit eigen beweging van de Commissie nr. 01/2013 van 21 januari 2013 *betreffende de na te leven veiligheidsmaatregelen ter voorkoming van gegevenslekken* (https://www.gegevensbeschermingsAutoriteit.be/sites/privacycommission/files/documents/aanbeveling_01_2013_0.pdf).

⁷ Referentiemaatregelen van de Commissie voor de beveiliging van elke verwerking van persoonsgegevens, Versie 1.0 (https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/referentiemaatregelen_voor_de_beviliging_van_elke_verwerking_van_persoonsgegevens_0.pdf).

⁸ Zie de aanbeveling nr. 01/2008 van 24 september 2008 *met betrekking tot het toegangs- en gebruikersbeheer in de overheidssector* (https://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_01_2008_0.pdf).

18. Ten slotte zal de AD Crisiscentrum van de FOD Binnenlandse Zaken toezien op de aanwijzing van een makkelijk bereikbaar aanspreekpunt (uitdrukkelijke vermelding op de website van het veiligheidsportaal) zodat de betrokkenen makkelijk hun aanvragen kunnen indienen om de rechten uit te oefenen waarover zij krachtens de wetgeving inzake de bescherming van persoonsgegevens beschikken.

OM DIE REDENEN,

de Autoriteit,

brengt een **gunstig advies** uit over het ontwerp van Koninklijk besluit op voorwaarde dat rekening wordt gehouden met de volgende opmerkingen:

1. Duidelijke vermelding van het doeleinde van de verplichte vermelding van de contactgegevens van personen in de ANIP, precieze bepaling van de categorieën van betrokkenen en de aard van de te vermelden gegevens en dit, overeenkomstig het beginsel van minimalisering van gegevens (punt 5) ;
2. Verplicht gebruik van generieke contactadressen voor de contactpersonen voor wie dit aangewezen is en het opleggen aan de betrokken overheden van de verplichte bijwerking van deze generieke contactadressen (punt 6) ;
3. Toevoeging van een definitie voor de begrippen deskundigen en actoren die specifiek betrokken zijn bij het risico, bedoeld in de artikelen 5,1°, a en 6,§1, 2° van het ontwerp en invoering van een opt-out voor sommigen onder hen (punten 7 en 8);
4. Herziening van de formulering van artikel 7 zoals aanbevolen in de punten 11 en 12.

Voor het overige **beveelt** de Autoriteit **aan** dat de FOD Binnenlandse Zaken zich schikt naar haar aanbevelingen vervat in de punten 12 tot 18 voor de parametrisering van zijn ICMS-veiligheidsportaal.

De Wnd. Administrateur,

De Voorzitter,

(get.) An Machtens

(get.) Willem Debeuckelaere